PCT/JP03/03974 #2

日本国特許庁
JAPAN PATENT OFFICE

28.03.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

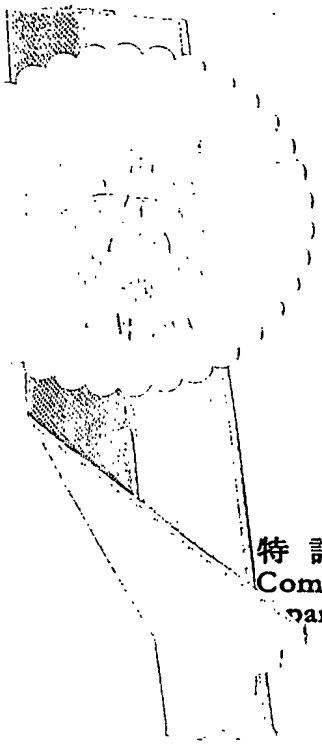
This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　４月　３日

出願番号
Application Number: 特願２００２－１０１７５６

[ST.10/C]: [ＪＰ２００２－１０１７５６]

出願人
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００３年　５月　９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３３８２４

【書類名】　特許願

【整理番号】　DCMH130719

【提出日】　平成14年 4月 3日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L　9/00

【発明の名称】　配信方法、配信システム及び端末装置

【請求項の数】　28

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　渡邊　信之

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　澤田　久徳

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　西尾　英昭

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　中村　友則

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　三浦　史光

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ

・ティ・ティ・ドコモ内

【氏名】　富岡　淳樹

【特許出願人】

【識別番号】　392026693

【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】　100098084

【弁理士】

【氏名又は名称】　川▲崎▼　研二

【選任した代理人】

【識別番号】　100111763

【弁理士】

【氏名又は名称】　松本　隆

【手数料の表示】

【予納台帳番号】　038265

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　配信方法、配信システム及び端末装置

【特許請求の範囲】

【請求項１】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、

前記端末装置が、前記配信システムから送信されてくるアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信されてくる前記セキュリティ記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程と

を有する配信方法。

【請求項２】　前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、

さらに、前記端末装置が、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する過程を有した

請求項１に記載の配信方法。

【請求項３】　前記配信システムは、セキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保する

請求項１に記載の配信方法。

【請求項４】　前記通信路は暗号化されている

請求項３に記載の配信方法。

【請求項５】　前記通信路は移動通信網および専用線により実現される

請求項３に記載の配信方法。

【請求項６】　前記通信路は移動通信網および暗号化された通信路により実現される

請求項３に記載の配信方法。

【請求項７】　前記セキュリティ記述ファイルに内包された権限情報は資源の利用に関する制限を示す

請求項１に記載の配信方法。

【請求項８】　前記資源は前記端末装置内部のハードウェア資源である

請求項７に記載の配信方法。

【請求項９】　前記資源は前記端末装置外部の、当該端末装置が使用可能なハードウェア資源である

請求項７に記載の配信方法。

【請求項１０】　前記資源は前記端末装置内部のソフトウェア資源である

請求項７に記載の配信方法。

【請求項１１】　前記資源は前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源である

請求項７に記載の配信方法。

【請求項１２】　前記資源は、前記端末装置が使用可能なネットワーク資源である

請求項７に記載の配信方法。

【請求項１３】　前記権限情報は資源の利用の種類を示す

請求項１に記載の配信方法。

【請求項１４】　前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、

前記端末装置は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する

請求項１に記載の配信方法。

【請求項１５】　前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記端末装置は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する

請求項１に記載の配信方法。

【請求項１６】　前記アプリケーション記述ファイルに記述された前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記端末装置は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する

請求項１に記載の配信方法。

【請求項１７】　前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記端末装置が、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから前記端末装置に対して当該セキュリティ記述ファイルが時系列的に繰り返し配信され、

さらに、前記端末装置は、繰り返し配信されてくる前記セキュリティ記述ファ

イルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する過程を有した

請求項１に記載の配信方法。

【請求項１８】　前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてこなかった場合には、前記アプリケーションの有効期限を更新しない

請求項１７に記載の配信方法。

【請求項１９】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有し、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知されると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する

配信システム。

【請求項２０】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置と

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記アプリケーション記述ファイルを格納した情報提供サーバ装置が、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、

前記端末装置が、前記送信されてくるアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記管理サーバ装置に通知し、

前記管理サーバ装置が、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信し、

前記端末装置が、前記管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を、前記実体ファイルを格納した情報提供サーバ装置に通知し、

前記実体ファイルを格納した情報提供サーバ装置が、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する

配信システム。

【請求項２１】　前記端末装置は移動機である

請求項２０に記載の配信システム。

【請求項２２】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムに対し、前記アプリケーション記述ファイルの格納位置を通知するアプリケーション位置通知手段と、

前記配信システムによって送信されてくる前記アプリケーション記述ファイル

を受信するアプリケーション情報受信手段と、

前記受信したアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するセキュリティ位置通知手段と、

前記配信システムによってセキュリティが確保された状態で送信されてくる前記セキュリティ記述ファイルを受信するセキュリティ情報手段と、

前記受信したセキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を前記配信システムに通知する実体位置通知手段と、

前記配信システムによって送信されてくる前記実体ファイルを受信する実体情報受信手段と

を有した端末装置。

【請求項２３】　前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは通信事業者の秘密鍵で署名されており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されている公開鍵を用いて、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルの正当性を検証する検証手段を有し、

前記実体通知手段は、前記検証手段によって正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する

請求項２２に記載の端末装置。

【請求項２４】　前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較する比較手段を有し、

前記実体位置通知手段は、前記比較手段によって両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する

請求項２２に記載の端末装置。

【請求項２５】　前記セキュリティ位置通知手段は、前記アプリケーション記述ファイルに内包された、前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する

請求項２２に記載の端末装置。

【請求項２６】　前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記セキュリティ位置通知手段が前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記セキュリティ情報受信手段は前記セキュリティ記述ファイルを時系列的に繰り返し受信し、

この繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する更新手段を有した

請求項２２に記載の端末装置。

【請求項２７】　前記更新手段は、前記配信システムから前記セキュリティ記述ファイルが正当に送信されてこなかった場合には、前記アプリケーションの有効期限を更新しない

請求項２６に記載の端末装置。

【請求項２８】　移動機であることを特徴とする請求項２２～２７のいずれか１に記載の端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、端末装置にアプリケーションを配信する技術に関する。

【０００２】

【従来の技術】

移動機の高機能化が急速に進みつつある。最近では、Ｊａｖａ（登録商標）プ

ログラミング言語に従って記述されたプログラムを含むソフトウェア（以下、Ｊａｖａ－ＡＰソフトウェアという）をネットワークを介してダウンロードし、これを実行してＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）を実現する機能を備えた移動機が開発されている。この種の移動機によるＪａｖａ－ＡＰソフトウェアのダウンロード手順は、まず、ＷＷＷ（World Wide Web）を構成するサーバ装置からＡＤＦ（Application Descriptor File）を取得し、次いでＪａｒ（Java Archive）ファイルを取得するという流れが通常である。

【０００３】

ＡＤＦはＪａｒファイルに依存した内容となっており、例えば、Ｊａｒファイルの格納位置を示すＵＲＬ（以下、パッケージＵＲＬという）、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等を必須情報として内包している。ＡＤＦを取得した移動機は、このＡＤＦの内容を参照するとともに自機の空きメモリ容量を確認する等して、ダウンロードしようとしているＪａｖａ－ＡＰソフトウェアを自機にインストール可能であるか否かを判断する。

【０００４】

インストール可能と判断すると、移動機は、ＡＤＦに内包されているパッケージＵＲＬを用いて、ＷＷＷを構成するサーバ装置からＪａｒファイルを取得する。このＪａｒファイルには、Ｊａｖａ－ＡＰソフトウェアが格納されており、Ｊａｒファイルの取得をもってＪａｖａ－ＡＰソフトウェアのダウンロードは完了する。以後、移動機において、ダウンロードされたＪａｖａ－ＡＰソフトウェアが起動可能に設定され、このＪａｖａ－ＡＰソフトウェアのインストールが完了する。

【０００５】

【発明が解決しようとする課題】

ところで、移動機内に実現されるＪａｖａ－ＡＰの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、Ｊａｖａ－ＡＰは、移動機内の電話帳データ等の秘匿性の高い情報を参照することができないように

なっている。このような制限の相違により、悪意をもって作成されたＪａｖａ－ＡＰ、あるいは不具合を有するＪａｖａ－ＡＰによって移動機内の秘匿性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができるようになっている。

【０００６】

しかし、上述した厳しい挙動制限を全てのＪａｖａ－ＡＰに対して一律に課すだけでは、Ｊａｖａ－ＡＰの高機能化や多様化を望むユーザやＩＰ（情報提供事業者）の意向に添うことができない。例えば、ある程度の信頼性が保証されるのであれば、移動機に格納された個人情報を参照する権限をＪａｖａ－ＡＰに与えてもよいと考えるユーザは少なくないと想定される。一方、ＩＰにも、移動機に格納されている個人情報や移動機が有する多数の機能の使用を前提とした、より魅力的なＪａｖａ－ＡＰを提供したいという要望がある。

【０００７】

これらの要望を満たす仕組みとして、移動機のユーザに対して通信サービスを提供する通信事業者等の、ユーザにとって信頼できる機関（以下、信頼機関という）が上述した挙動制限を緩和した権限をＪａｖａ－ＡＰに与え、この権限を移動機に通知し、移動機はこの権限に基づいてＪａｖａ－ＡＰの挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

【０００８】

Ｊａｖａ－ＡＰソフトウェアのダウンロード手順に上述の仕組みを適用する場合、ＡＤＦあるいはＪａｒファイルに権限を示す情報を内包させるのが妥当である。とりわけ、ＪａｒファイルはＩＰにより随時更新される種類のファイルであってＩＰが保有するのが適当であることから、信頼機関に保有させるならＡＤＦが妥当ということになる。

【０００９】

しかしながら、ＡＤＦはＪａｒファイルに依存した内容となることから、ＩＰが手元のＪａｒファイルを更新すると、信頼機関が保有しているＡＤＦの更新も必要になってくる。信頼機関は他者の関与を排するようにＡＤＦを管理すること

が必要であるから、信頼機関とＩＰが連携してＡＤＦを更新する作業は繁雑なものとなることが懸念される。

また、Ｊａｒファイルを更新せずとも、ＡＤＦの更新が必要となることがある。例えば、ＩＰにおいて、あるＪａｒファイルへのアクセスが集中し、このＪａｒファイルを他のサーバ装置へ移動する場合である。この場合、Ｊａｒファイルの格納位置が変更されるから、ＡＤＦに内包されているパッケージＵＲＬを変更する必要がある。この場合においても、上記のような懸念は当然生じ得る。

【００１０】

本発明は、上述した事情に鑑みて為されたものであり、権限に応じた挙動をアプリケーションに許可する端末装置に対し、依存関係にある複数のファイルを配信することによってそのアプリケーションを実現するためのソフトウェアを配信可能な仕組みを提供することを目的としている。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムが、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信する過程と、

前記端末装置が、前記取得したアプリケーション記述ファイルに内包されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前

記端末装置に送信する過程と、

前記端末装置が、前記配信システムから送信されてくる前記セキュリティ記述ファイルに内包されている前記実体ファイルの格納位置を前記配信システムに通知する過程と、

前記配信システムが、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する過程と

を有する配信方法を提供する。

この方法によれば、配信システムが、アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、得したアプリケーション記述ファイルに内包されているセキュリティ記述ファイルの格納位置を配信システムに通知し、配信システムが、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装置が、配信システムから送信されてくるセキュリティ記述ファイルに内包されている実体ファイルの格納位置を前記配信システムに通知し、配信システムが、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

【００１２】

この場合において、前記配信システムは、前記セキュリティ記述ファイルを暗号化して前記端末装置に送信することによってセキュリティを確保しており、

さらに、前記端末装置が、前記配信システムによって送信されてくる暗号化されたセキュリティ記述ファイルを復号化する過程を有していてもよい。

【００１３】

また、前記配信システムはセキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保してもよい。

この場合、前記通信路は暗号化されていてもよいし、移動通信網および専用線により実現されていてもよいし、移動通信網および暗号化された通信路により実現されていてもよい。

【００１４】

また、前記セキュリティ記述ファイルに内包された権限情報は資源の利用に関する制限を示す情報であってもよい。この場合、資源は、前記端末装置内部のハードウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なハードウェア資源であってもよいし、前記端末装置内部のソフトウェア資源であってもよいし、前記端末装置外部の、当該端末装置が使用可能なソフトウェア資源であってもよいし、前記端末装置が使用可能なネットワーク資源であってもよい。

【００１５】

また、前記セキュリティ記述ファイルに内包された権限情報は資源の利用の種類を示す情報であってもよい。

【００１６】

好ましい態様において、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは前記通信事業者の秘密鍵で署名されており、

前記端末装置は、前記配信システムによって送信されてくるセキュリティ記述ファイルの正当性を前記アプリケーション記述ファイルに内包されている公開鍵を用いて検証し、その正当性が検証された場合にのみ、前記配信システムに対し前記実体ファイルの格納位置を通知する。

【００１７】

好ましい態様において、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記端末装置は、前記配信システムによって送信されてくるアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記配信システムによって送信されてくるセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する。

【００１８】

好ましい態様において、前記アプリケーション記述ファイルに記述された前記

セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記端末装置は、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知してもよい。

【００１９】

好ましい態様において、前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記端末装置が、前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記配信システムから前記端末装置に対して当該セキュリティ記述ファイルが時系列的に繰り返し配信され、

さらに、前記端末装置は、繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する過程を有している。

【００２０】

この場合において、前記端末装置は、前記配信システムから前記セキュリティ記述ファイルが正当に配信されてこなかった場合には、前記アプリケーションの有効期限を更新しないようにしてもよい。

【００２１】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有し、

各々の前記サーバ装置は、ファイルの格納位置が通知されると当該ファイルをその通知元に返送し、

前記管理サーバ装置は、前記セキュリティ記述ファイルの格納位置が通知され

ると当該セキュリティ記述ファイルをセキュリティが確保された状態で通知元に返送する

配信システムを提供する。

このシステムによれば、アプリケーション記述ファイルの格納位置が通知されると、その通知元に対して当該アプリケーション記述ファイルを送信し、セキュリティ記述ファイルの格納位置が通知されると、その通知元に対してセキュリティ記述ファイルをセキュリティが確保された状態で通知元に送信し、実体ファイルの格納位置が通知されると、その実体ファイルを通知元に送信する。

【００２２】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、

前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置と

前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記アプリケーション記述ファイルを格納した情報提供サーバ装置が、前記アプリケーション記述ファイルの格納位置を前記端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、

前記端末装置が、前記送信されてくるアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記管理サーバ装置に通知し、

前記管理サーバ装置が、前記通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で前記端末装置に送信し、

前記端末装置が、前記管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を、前記実体ファイルを格納した情報提供サーバ装置に通知し、

前記実体ファイルを格納した情報提供サーバ装置が、前記通知された実体ファイルの格納位置に基づいて、当該実体ファイルを前記端末装置に送信する

配信システムを提供する。

このシステムによれば、アプリケーション記述ファイルを格納した情報提供サーバ装置が、アプリケーション記述ファイルの格納位置を端末装置によって通知されると、当該端末装置に対して当該アプリケーション記述ファイルを送信し、端末装置が、送信されてくるアプリケーション記述ファイルに記述されているセキュリティ記述ファイルの格納位置を管理サーバ装置に通知し、管理サーバ装置が、通知されたセキュリティ記述ファイルの格納位置に基づいて、当該セキュリティ記述ファイルをセキュリティが確保された状態で端末装置に送信し、端末装置が、管理サーバ装置から送信されてくる前記セキュリティ記述ファイルに記述されている実体ファイルの格納位置を、実体ファイルを格納した情報提供サーバ装置に通知し、実体ファイルを格納した情報提供サーバ装置が、通知された実体ファイルの格納位置に基づいて、当該実体ファイルを端末装置に送信する。

【００２３】

この場合において、前記端末装置は移動機であれば望ましい。

【００２４】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報を内包したセキュリティ記述ファイルを格納した管理サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置と前記セキュリティ記述ファイルの格納位置とが記述されたアプリケーション記述ファイルを格納した情報提供サーバ装置とを有した配信システムに対し、前記アプリケーション記述ファイルの格納位置を通知するアプリケーション位置通知手段と、

前記配信システムによって送信されてくる前記アプリケーション記述ファイル

を受信するアプリケーション情報受信手段と、

前記受信したアプリケーション記述ファイルに記述されている前記セキュリティ記述ファイルの格納位置を前記配信システムに通知するセキュリティ位置通知手段と、

前記配信システムによってセキュリティが確保された状態で送信されてくる前記セキュリティ記述ファイルを受信するセキュリティ情報手段と、

前記受信したセキュリティ記述ファイルに記述されている前記実体ファイルの格納位置を前記配信システムに通知する実体位置通知手段と、

前記配信システムによって送信されてくる前記実体ファイルを受信する実体情報受信手段と

を有した端末装置を提供する。

この端末装置によれば、アプリケーション位置通知手段が、アプリケーション記述ファイルの格納位置を配信システムに通知し、アプリケーション情報受信手段が、配信システムによって送信されてくるアプリケーション記述ファイルを受信し、セキュリティ位置通知手段が、受信したアプリケーション記述ファイルに記述されているセキュリティ記述ファイルの格納位置を前記配信システムに通知し、セキュリティ情報受信手段が、配信システムによってセキュリティが確保された状態で送信されてくるセキュリティ記述ファイルを受信し、実体位置通知手段が、受信したセキュリティ記述ファイルに記述されている実体ファイルの格納位置を前記配信システムに通知し、実体情報受信手段が、配信システムによって送信されてくる実体ファイルを受信する。

【００２５】

好ましくは、前記アプリケーション記述ファイルは前記端末装置に通信サービスを提供する通信事業者の公開鍵を内包し、

前記セキュリティ記述ファイルは通信事業者の秘密鍵で署名されており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されている公開鍵を用いて、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルの正当性を検証する検証手段を有し、

前記実体通知手段は、前記検証手段によって正当性が検証された場合にのみ、

前記配信システムに対し前記実体ファイルの格納位置を通知する。

【００２６】

好ましくは、前記アプリケーション記述ファイル及び前記セキュリティ記述ファイルは、対応するアプリケーションに割り当てられたアプリケーション識別子を内包しており、

前記アプリケーション情報受信手段によって受信したアプリケーション記述ファイルに内包されたアプリケーション識別子と、前記セキュリティ情報受信手段によって受信したセキュリティ記述ファイルに内包されたアプリケーション識別子とを比較する比較手段を有し、

前記実体位置通知手段は、前記比較手段によって両者が一致した場合にのみ、前記配信システムに前記実体ファイルの格納位置を通知する。

【００２７】

好ましくは、前記セキュリティ位置通知手段は、前記アプリケーション記述ファイルに内包された、前記セキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ、前記セキュリティ記述ファイルの格納位置を前記配信システムに通知する。

【００２８】

好ましくは、前記セキュリティ記述ファイルは、対応するアプリケーションの有効期限を示す期限情報を内包しており、

前記セキュリティ位置通知手段が前記配信システムに対して前記セキュリティ記述ファイルの格納位置を時系列的に繰り返し通知することによって、前記セキュリティ情報受信手段は前記セキュリティ記述ファイルを時系列的に繰り返し受信し、

この繰り返し配信されてくる前記セキュリティ記述ファイルに内包されている前記期限情報に基づいて、前記アプリケーションの有効期限を更新する更新手段を有している。

【００２９】

この場合において、前記更新手段は、前記配信システムから前記セキュリティ記述ファイルが正当に送信されてこなかった場合には、前記アプリケーションの

有効期限を更新しないようにしてもよい。

【００３０】

なお、上記の場合において、前記端末装置は移動機であれば望ましい。

【００３１】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の一形態である配信システムについて図面を参照して説明する。なお、図面において、共通する部分には同一の符号が付されている。

この配信システムは、移動通信網を管理する通信事業者（即ち信頼できる機関）が、移動機にインストール可能なＪａｖａ－ＡＰソフトウェアをダウンロードするための情報を移動機のユーザへ提示し、この提示を受けたユーザが、移動機を操作して所望のＪａｖａ－ＡＰソフトウェアを移動機にダウンロードおよびインストールし、移動機において起動するためのものである。

【００３２】

本システムにおけるＪａｖａ－ＡＰソフトウェアのダウンロードは、まず、Ｊａｖａ－ＡＰソフトウェアの内容を説明した画面を移動機において表示した後、この移動機のユーザが所望するＪａｖａ－ＡＰソフトウェアに対応したＡＤＦを移動機に配信し、次いで、上記Ｊａｖａ－ＡＰソフトウェアに対応したＳＤＦ（セキュリティ記述ファイル）と称せられるファイルを移動機に配信し、最後にＪａｒファイルを移動機に配信するという手順で行われる。ここで、ＳＤＦは、トラステッドＡＰＩ（APplication Interface；詳しくは後述する）を使用するＪａｖａ－ＡＰを移動機において実現するためのＪａｖａ－ＡＰソフトウェアを移動機にダウンロードする際に必須のファイルであって、移動機内におけるＪａｖａ－ＡＰソフトウェアの挙動を制限する内容が記述されたファイルである。よって、移動機は、インストールしたＪａｖａ－ＡＰソフトウェアを実行するに際しては、このＳＤＦの記述内容に従うこととなる。このＳＤＦは、Ｊａｖａ－ＡＰソフトウェアについて上記通信事業者とこのＪａｖａ－ＡＰソフトウェアを提供するＩＰとの間で結ばれた契約に従って通信事業者により作成される。

【００３３】

（１）構成

図１に示されるように、この配信システムは、インターネット１１に接続されたＩＰサーバ装置１２～１４と、通信事業者が移動パケット通信サービスを提供するために用いる移動パケット通信網１５と、この移動パケット通信網１５との間で無線パケット通信を行ってこの移動パケット通信網１５を介して通信相手とパケット通信を行う移動機１６と、インターネット１１と移動パケット通信網１５とを相互接続するゲートウェイサーバ装置１７と、専用線によりゲートウェイサーバ装置１７に接続された管理サーバ装置１８とを有する。この配信システムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機１６のみが図示されている。これと同様の理由により、３つのＩＰサーバ装置１２～１４のみが図示されている。

【００３４】

以下、この配信システムの各構成要素について詳細に説明する。

（１－１）ＩＰサーバ装置

ＩＰサーバ装置１２は第１のＩＰに管理されており、ＩＰサーバ装置１３および１４は第１のＩＰと異なる第２のＩＰにより管理されている。ＩＰサーバ装置１２～１４はＷＷＷを構成しており、それぞれ一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。また、ＩＰサーバ装置１２は不揮発性メモリ１２Ａ、ＩＰサーバ装置１３は不揮発性メモリ１３Ａ、ＩＰサーバ装置１４は不揮発性メモリ１４Ａを有し、ＩＰサーバ装置１２～１４はそれぞれ、ＴＣＰに従ったコネクション（以後、ＴＣＰコネクション）を通信相手との間に確立し、このコネクションを介してＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを受信すると、このＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを自身の不揮発性メモリから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送してこのコネクションを切断する。

【００３５】

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａはそれぞれハードディスク等の不揮発性メモリであり、Ｊａｖａプログラミング言語を用いて作成されたプログラムを内包するＪａｒファイルと、このＪａｒファイルに関する情報を記述したＡ

ＤＦと、このプログラムを内包するＪａｖａ－ＡＰソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶し得る。ＩＰサーバ装置１２～１４の各々は、対応するＩＰの指示に従って上記各ファイルを作成および更新する機能を備えている。

【００３６】

ところで、本実施形態では、対応するＳＤＦが存在するＪａｖａ－ＡＰソフトウェアと、対応するＳＤＦが存在しないＪａｖａ－ＡＰソフトウェアとが用意されている。前者のＪａｖａ－ＡＰソフトウェアは、対応するＳＤＦに記述された挙動制限を受けるものであり、通信事業者がＩＰとの契約に基づいて信頼性を保証したものであることから「トラステッドＪａｖａ－ＡＰソフトウェア」と呼び、後者を「非トラステッドＪａｖａ－ＡＰソフトウェア」と呼ぶ。ＩＰサーバ装置に格納され得るＡＤＦには、トラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦと、非トラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦとがある。これらのいずれもＡＤＦにおいても、Ｊａｖａ－ＡＰの名称や、ＷＷＷにおけるＪａｒファイルの記憶位置を示すパッケージＵＲＬや、Ｊａｒファイルのサイズを示す情報や、Ｊａｒファイルの最終変更日時を示す情報等の、従来からＡＤＦに内包されている情報が記述されている。これに加えて、トラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦは、上記のパッケージＵＲＬ等の他、図２に示されるように、トラステッドＪａｖａ－ＡＰソフトウェアを一意に識別するためのＡＰＩＤと、Ｊａｒファイルのハッシュ値と、ＳＤＦがＷＷＷにおいて記憶されている位置を示すＵＲＬ（以下、ＳＤＦ－ＵＲＬと呼ぶ）と、図示せぬＣＡ（認証局）によって証明された通信事業者の公開鍵とを内包している。

【００３７】

次に、説明ファイルはＨＴＭＬに従って記述されるテキストファイルであり、移動機においてＨＴＭＬに従って解釈されたときに、このファイルに対応するＪａｖａ－ＡＰソフトウェアをダウンロードするときにユーザにより操作されるオブジェクトとこのＪａｖａ－ＡＰソフトウェアに対応するＡＤＦがＷＷＷにおいて記憶されている位置を示すＵＲＬとが対応付けられたＵＩ（ユーザインターフ

エイス、以下同じ）が提供されるように記述されている。

【００３８】

（１－２）ゲートウェイサーバ装置

ゲートウェイサーバ装置１７は前述の通信事業者により管理されており、移動パケット通信網１５とインターネット１１とを接続する一般的なゲートウェイサーバ装置と同様の構成を有し、移動パケット通信網１５とインターネット１１と管理サーバ装置１８との間で相互に通信を中継する。

【００３９】

（１－３）管理サーバ装置

管理サーバ装置１８は前述の通信事業者により管理されており、ＷＷＷを構成し、一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。また、管理サーバ装置１８はハードディスク等の不揮発性メモリ１８Ａを有し、ＴＣＰコネクションを通信相手との間に確立し、このコネクションを介してＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを受信すると、このＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを不揮発性メモリ１８Ａから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送してこのコネクションを切断する。

【００４０】

不揮発性メモリ１８Ａに記憶されるファイルとしては、移動機１６にダウンロード可能なＪａｖａ－ＡＰソフトウェアを移動機１６のユーザに紹介するためのリストファイル２００と、複数のトラステッドＪａｖａ－ＡＰソフトウェアにそれぞれ対応した複数のＳＤＦとがある。

リストファイル２００はＨＴＭＬに従って記述されたテキストファイルであり、ＨＴＭＬに従って解釈された場合に、Ｊａｖａ－ＡＰソフトウェア毎に対応した選択肢と、このＪａｖａ－ＡＰソフトウェアの説明ファイルがＷＷＷにおいて記憶されている位置を示すＵＲＬとが対応付けられたＵＩが提供されるように記述されている。

【００４１】

ＳＤＦは、トラステッドＡＰソフトウェア毎に通信事業者により作成されるフ

ァイルであり、図３に示されるように、トラステッドＪａｖａ－ＡＰソフトウェアを一意に識別するためのＡＰＩＤと、このトラステッドＪａｖａ－ＡＰソフトウェアの移動機１６における挙動制限を示すポリシー情報と、このトラステッドＪａｖａ－ＡＰソフトウェアの有効期限とを内包しており、さらに、これらが通信事業者の秘密鍵によって署名されている。このＳＤＦは、上述したＡＤＦに格納されている公開鍵で復号化されることにより、その正当性が確認されることとなる。

【００４２】

ＳＤＦ内のポリシー情報は、例えば図４に概念的に示されるように、トラステッドＡＰＩの名称と、そのトラステッドＡＰＩに対する挙動制限を示したパーミッションとが対応付けられた内容となっている。図４に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドＡＰＩである“getPhoneList()”と移動機の状態を取得するときに必須のトラステッドＡＰＩである“getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドＡＰＩである“getCallHistory()”の使用が禁止されている。

【００４３】

（１－４）移動機

移動機１６は、図５に示されるように、ＯＳ（オペレーティングシステム）ソフトウェア、Ｊａｖａ－ＡＰを実行する環境を構築するためのＪａｖａ－ＡＰ環境ソフトウェア、および各種ネイティブＡＰソフトウェア等を記憶したＲＯＭ１６Ａと、ＲＯＭ１６Ａからプログラムを読み出して実行するＣＰＵ１６Ｂと、表示部１６Ｃと、不揮発性メモリ１６Ｄと、ＲＡＭ１６Ｅと、通信部１６Ｆと、操作部１６Ｇと、計時部１６Ｈとを有し、これらは通信線によって接続されている。

【００４４】

表示部１６Ｃは、例えば液晶表示パネルやパネル駆動回路を有し、ＣＰＵ１６Ｂから供給されるデータで表される画像を表示する。

不揮発性メモリ１６Ｄは例えばＳＲＡＭ（Static Random Access Memory）

やＥＥＰＲＯＭ（Ellectrically Erasable and Programmable Read Only Memory）である。また、この不揮発性メモリ１６Ｄは、ＷＷＷを構成するサーバ装置からダウンロードしたＪａｖａ－ＡＰソフトウェアを記憶するために使用される。

なお、本実施形態の説明において「Ｊａｖａ－ＡＰソフトウェア」と言う場合には、それが「トラステッドＪａｖａ－ＡＰソフトウェア」であればＡＤＦ、ＳＤＦ及びＪａｒファイルを含む概念とし、「非トラステッドＪａｖａ－ＡＰソフトウェア」であればＡＤＦ及びＪａｒファイルを含む概念とする。

【００４５】

通信部１６Ｆは、アンテナや無線送受信部を備え、移動パケット通信網１５と無線パケット通信を行うものであり、ＣＰＵ１６Ｂと移動パケット通信網１５との間でパケットを中継する。また、通信部１６Ｆは、通話のためのＣＯＤＥＣやマイク、スピーカ等をも備えており、これによって移動機１６は図示せぬ移動電話網を介して回線交換による通話を行うこともできる。

操作部１６Ｇは操作子を備え、操作子の操作に応じた信号をＣＰＵ１６Ｂへ供給する。

計時部１６Ｈは現在の年月日及び時刻（以下、単に現在日時という）を計時する。なお、計時部１６Ｈがより正確な現在日時を計時するためには、例えば移動パケット通信網１５の図示せぬ基地局から制御チャネルを用いて定期的に通知される現在日時に同期させるような処理を行ってもよい。

【００４６】

さて、移動機１６の図示せぬ電源が投入されると、ＣＰＵ１６ＢはＲＡＭ１６Ｅをワークエリアとし、ＲＯＭ１６ＡからＯＳソフトウェアに内包されているプログラムを読み出して実行する。これにより、ＣＰＵ１６ＢにはＵＩ等を提供する機能が実現される。すなわち、ＣＰＵ１６ＢはＯＳソフトウェアを起動して移動機１６内にて図６に示すＯＳを実現する。ＯＳは操作部１６Ｇから供給される信号とＵＩの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

【００４７】

例えば、ユーザの指示がネイティブＡＰソフトウェアである通信ソフトウェアの起動を要求するものであれば、ＯＳは通信ソフトウェアを起動して移動機１６内にて通信ＡＰを実現する。この通信ＡＰを用いることで、ユーザは通話相手と通話をすることができる。

【００４８】

また、ユーザの指示がネイティブＡＰソフトウェアである電話帳ソフトウェアの起動を要求するものであれば、ＯＳは電話帳ソフトウェアを起動して移動機１６内にて電話帳ＡＰを実現する。この電話帳ＡＰを用いることで、ユーザは、不揮発性メモリ１６Ｄに記憶された電話帳の内容を示すデータ（以後、電話帳データという）を参照・使用・変更することができる。

【００４９】

また、ユーザの指示がネイティブＡＰソフトウェアであるＷｅｂブラウザソフトウェアの起動を要求するものであれば、ＯＳはＷｅｂブラウザソフトウェアを起動して移動機１６内にてＷｅｂブラウザを実現する。ＷｅｂブラウザはＵＩを提供し、このＵＩの状態と操作部１６Ｇから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、この指示がユーザによって指定されたファイルをWWWから取得する旨の場合には、通信部１６Ｆを制御してこのファイルを記憶したＩＰサーバ装置との間にＴＣＰコネクションを確立し、このコネクションを介して、指定された位置を示すＵＲＬをＧＥＴメソッドに指定したＨＴＴＰの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、このコネクションを切断する。さらに、Ｗｅｂブラウザは、受信した応答メッセージに内包されているファイルをＨＴＭＬに従って解釈し、Ｗｅｂページを内包するＵＩを生成し、ユーザに提供する。また、ユーザの指示がＪａｖａ－ＡＰソフトウェアのダウンロードを要求するものである場合には、Ｗｅｂブラウザは、この指示を次に述べるＪＡＭ（Java Application Manager）に通知する。より具体的には、Ｗｅｂページにおいて、オブジェクトタグが指定されているアンカータグで表されるアンカーが押下（クリック操作またはプレス操作）されると、Ｗｅｂブラウザはこのオブジェクトタグのｄａｔａ属性に指定されているＵＲＬを抽出し、このＵＲＬからのＪａｖａ－ＡＰソフトウ

ェアのダウンロードが要求されたことをＪＡＭに通知する。

【００５０】

また、ユーザの指示がネイティブＡＰソフトウェアであるＪＡＭソフトウェアの起動を要求するものであれば、ＯＳはＪＡＭソフトウェアを起動して移動機１６内にてＪＡＭを実現する。ＪＡＭは、移動機１６にインストールされているＪａｖａ－ＡＰソフトウェアの一覧をユーザに提示し、ユーザにより指定されたＪａｖａ－ＡＰソフトウェアを起動する。具体的には、ＪＡＭに対するユーザの指示がＪａｖａ－ＡＰソフトウェアの起動を要求するものであれば、Ｊａｖａ－ＡＰ環境ソフトウェアが起動されて移動機１６内にＪａｖａ－ＡＰ環境が実現され、次に、指定されたＪａｖａ－ＡＰソフトウェアが起動されてＪａｖａ－ＡＰ環境内にＪａｖａ－ＡＰが実現される。Ｊａｖａ－ＡＰ環境は、移動機１６のような携帯端末に適した軽量のＪａｖａ仮想マシンであるＫＶＭ（K Vartual Machine）と、Ｊａｖａ－ＡＰに対して提供されるＡＰＩ（Application Interface）とを有する。Ｊａｖａ－ＡＰに対して提供されるＡＰＩは、トラステッドＪａｖａ－ＡＰソフトウェアによって実現されるＪａｖａ－ＡＰ（以後、トラステッドＪａｖａ－ＡＰという）のみに使用が許可されるトラステッドＡＰＩと、あらゆるＪａｖａ－ＡＰに使用が許可される非トラステッドＡＰＩとに分けられる。

【００５１】

次に、移動機１６が備える機能について説明する。

（１－４－１）移動機１６によるＪａｖａ－ＡＰソフトウェアのダウンロード機能

ＪＡＭは、Ｊａｖａ－ＡＰソフトウェアのダウンロードを要求する指示がＷｅｂブラウザから通知されると、Ｊａｖａ－ＡＰソフトウェアを移動機１６にダウンロードしインストールする処理を行う。この処理の流れを図７に示す。

図７に示されるように、ＪＡＭは、Ｊａｖａ－ＡＰソフトウェアのダウンロードを要求する指示がＷｅｂブラウザから通知されると（ステップＳ１１；Ｙｅｓ）、

ダウンロードしようとするＪａｖａ－ＡＰソフトウェアに対応するＡＤＦをＩＰサーバ装置１２～１４のいずれかから取得する（ステップＳ１２）。具体的には

、ＪＡＭは、ＩＰサーバ装置１２～１４との間にＴＣＰコネクションを確立し、このＡＤＦの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＡＤＦを取得した後、このＴＣＰコネクションを切断する。そして、ＪＡＭは、応答メッセージに内包されているＡＤＦを不揮発性メモリ１６Ｄに書き込む。

【００５２】

次いで、ＪＡＭは、ダウンロードしようとしているＪａｖａ－ＡＰソフトウェアを移動機１６にインストール可能か否かをＡＤＦの内容に基づいて判定する（ステップＳ１３）。ここでは、ＡＤＦに記述されていたＪａｒファイルのサイズと、不揮発性メモリ１６Ｄ内のＪａｒファイルを記憶可能な空き容量とを比較する等の、従来と同様の基準に従って判定すればよい。

【００５３】

ここで、インストール可能と判定された場合には（ステップＳ１３；Ｙｅｓ）、ＪＡＭは、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアであるか否かを判定する（ステップＳ１４）。具体的には、ＪＡＭは、ステップＳ１２において取得したＡＤＦ内にＳＤＦ－ＵＲＬが記述されているか否かを確認し、記述されていれば、このＪａｖａ－ａｐソフトウェアに対応するＳＤＦが存在する、即ち、トラステッドＪａｖａ－ＡＰソフトウェアであると判定するし、その記述がなければ非トラステッドＪａｖａ－ＡＰソフトウェアであると判定する。

【００５４】

そして、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアが非トラステッドＪａｖａ－ＡＰソフトウェアであると判定された場合には（ステップＳ１４；Ｎｏ）、従来と同様のダウンロードおよびインストール処理が行われる（ステップＳ１５）。

【００５５】

一方、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアと判定された場合には（ステップＳ１４；Ｙｅｓ）、ＪＡＭは、このソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得

する（ステップＳ１６）。すなわち、ＪＡＭは、管理サーバ装置１８との間にＴＣＰコネクションを確立し、このコネクションを介して、ＡＤＦ内に記述されているＳＤＦ－ＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＳＤＦを取得した後、上記コネクションを切断する。

【００５６】

前述したように、トラステッドＪａｖａ－ＡＰソフトウェアに対応するＳＤＦは、ＡＰＩＤとポリシー情報と有効期限とを内包し、さらに通信事業者の秘密鍵により署名（暗号化）されている。そこで、ＪＡＭは、応答メッセージに内包されているＳＤＦの署名を、既に取得しているＡＤＦから抽出された公開鍵を用いて検証し（復号し）、このＳＤＦの正当性を判断する（ステップＳ１７）。正当性が確認された場合（ステップＳ１７；Ｙｅｓ）、ＪＡＭは、ＳＤＦを不揮発性メモリ１６Ｄに書き込む。

【００５７】

次いで、ＪＡＭは、ＳＤＦに内包されているＡＰＩＤと、既に取得しているＡＤＦに内包されていたＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ１８）。

両者が一致すると判定された場合には（ステップＳ１８；Ｙｅｓ）、ＪＡＭは、Ｊａｒファイルを取得する（ステップＳ１９）。具体的には、ＪＡＭは、ＡＤＦに内包されているパッケージＵＲＬで特定されるＪａｒファイルを記憶したＩＰサーバ装置１２～１４のいずれかとの間にＴＣＰコネクションを確立し、このＪａｒファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＪａｒファイルを取得し、このＴＣＰコネクションを切断する。

【００５８】

次に、ＪＡＭは、取得したＪａｒファイルに対するハッシュ値を算出する（ステップＳ２０）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機１６で使用されるハッシュ関数とＡＤＦに含まれるハッシュ値の算出時に使用されるハッシュ関数とは一致していなければならない。実際には、移動機１６

で使用されるハッシュ関数を用いて、トラステッドＪａｖａ－ＡＰソフトウェアを提供するＩＰがハッシュ値を算出してＡＤＦを生成することになる。

【００５９】

ＪＡＭは、算出したハッシュ値とＡＤＦから抽出したハッシュ値とを比較し、両者が一致した場合には（ステップＳ２１；Ｙｅｓ）、取得したＪａｒファイルを不揮発性メモリ１６Ｄに書き込み、トラステッドＪａｖａ－ＡＰソフトウェアのインストールに係る各種処理を行い（ステップＳ２２）、インストールに成功した旨をユーザに通知する（ステップＳ２３）。

以降、ＪＡＭは、トラステッドＪａｖａ－ＡＰソフトウェアを実行するに際し、トラステッドＪａｖａ－ＡＰの挙動を監視し、トラステッドＡＰＩの使用を制限するが、この制限は不揮発性メモリ１６Ｄに記憶されるＳＤＦ内のポリシー情報に従って行われることとなる。

【００６０】

なお、Ｊａｖａ－ＡＰソフトウェアをインストール不可能と判断された場合（ステップＳ１３；Ｎｏ）、ＳＤＦが正当でないと判断した場合（ステップＳ１７；Ｎｏ）、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合（ステップＳ１８；Ｎｏ）、算出したハッシュ値とＡＤＦが有するハッシュ値とが不一致の場合（ステップＳ２１；Ｎｏ）には、ＪＡＭは、インストールに失敗した旨をユーザに通知するとともに、移動機１６の状態をステップＳ１１以前の状態に戻す。

【００６１】

（１－４－２）移動機１６によるＳＤＦの更新機能

ところで、トラステッドＪａｖａ－ＡＰソフトウェアは、対応するＳＤＦに内包されていた有効期限が経過するまでは移動機１６によって実行可能である。この有効期限を更新する場合には、移動機１６は、管理サーバ１８から新たにＳＤＦを取得する必要がある。そこで、以下では、ＪＡＭが、ＳＤＦ内の有効期限が到来する度にその有効期限を更新する場合の処理について、図８に示すフローを参照しながら説明する。

【００６２】

図８に示されるように、ＪＡＭは、移動機１６内の計時部１６Ｈによって計時される現在日時と、今までに取得した全てのＳＤＦからそれぞれ抽出して不揮発性メモリ１６Ｄに記憶した複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している（ステップＳ３１）。

【００６３】

いずれか１つでも有効期限が到来すると（ステップＳ３１；Ｙｅｓ）、ＪＡＭは、有効期限が到来したＪａｖａ－ＡＰソフトウェアの名称とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部１６Ｃに表示してユーザの操作があるまで待機する。

ユーザが有効期限を更新することを指示する操作を行うと、ＪＡＭはこの指示内容を解釈し（ステップＳ３２；Ｙｅｓ）、この有効期限を更新すべきＪａｖａ－ＡＰソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得する（ステップＳ３３）。具体的には、ＪＡＭは、不揮発性メモリ１６Ｄの記憶内容を参照し、有効期限を更新すべきＪａｖａ－ＡＰソフトウェアのＡＰＩＤを内包したＡＤＦに内包されているＳＤＦ－ＵＲＬを抽出し、このＳＤＦ－ＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信してＳＤＦを取得した後、上記コネクションを切断する。

【００６４】

次いで、ＪＡＭは、上記ＳＤＦ－ＵＲＬを用いてＳＤＦを取得できたか否かを判断する（ステップＳ３４）。ここで、ＳＤＦを取得できない場合とは、何らかの事情でＪａｖａ－ＡＰソフトウェアの使用を中断或いは中止させたいという理由から、通信事業者が、管理サーバ装置１８において上記のＳＤＦ－ＵＲＬによって示される位置にＳＤＦを記憶させていないことを意味している。その事情とは、例えば、ＩＰの都合によってＪａｖａ－ＡＰソフトウェアの使用を中止或いは中断させたい場合（例えば、ユーザが一定期間だけ試用できるソフトウェアを配信するような場合）や、ＩＰと通信事業者との間で締結されていた契約が失効した場合等である。

【００６５】

さて、ＪＡＭは、ＳＤＦの取得に成功すると（ステップＳ３４；Ｙｅｓ）、ＳＤＦの署名を、既に取得しているＡＤＦに内包されている公開鍵を用いて検証し（復号し）、このＳＤＦの正当性を判断する（ステップＳ３５）。

【００６６】

正当性が確認されると（ステップＳ３５；Ｙｅｓ）、ＪＡＭは、ＳＤＦに内包されているＡＰＩＤと、既に取得済みのＡＤＦに内包されているＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ３６）。両者が一致すると判定された場合には（ステップＳ３６；Ｙｅｓ）、ＪＡＭは、取得したＳＤＦを不揮発性メモリ１６Ｄに既に書き込まれている以前のＳＤＦに上書きし、これにより有効期限を更新する。

【００６７】

なお、ユーザの操作により有効期限を更新しないと判断された場合（ステップＳ３２；Ｎｏ）、ＳＤＦを取得できなかった場合（ステップＳ３４；Ｎｏ）、ＳＤＦが正当でないと判断した場合（ステップＳ３５；Ｎｏ）、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合（ステップＳ３６；Ｎｏ）、ＪＡＭは、有効期限を更新しない旨をユーザに通知するとともに、移動機１６の状態をステップＳ３１以前の状態に戻す。

【００６８】

（２）動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、ＴＣＰコネクションの確立および切断動作についてはＨＴＴＰにおける一般的な動作となることから、それらの説明を省略する。また、前述のＯＳ、Ｗｅｂブラウザ、ＪＡＭ、Ｊａｖａ－ＡＰ、ネイティブＡＰ等が行う動作は移動機１６の動作となることから、以降の説明では、動作の主体を移動機１６とする。

【００６９】

また、図９に示されるように、管理サーバ装置１８の不揮発性メモリ１８Ａには、リストファイル２００とＳＤＦ２０４が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰと管理サーバ装

置１８を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されている。

これらのうち、リストファイル２００は、移動機１６において解釈・実行されると図１０に示されるリストページ２０１を提供するように記述されている。また、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ａが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０２のＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ｂが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０７のＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

【００７０】

また、ＳＤＦ２０４は、ＡＰＩＤとして“0001”、ポリシー情報として図４に示される内容の情報、有効期限として“２００２年１０月１日午前１０時”を内包しており、これらは通信事業者の秘密鍵を用いて署名されている。

【００７１】

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「詰め将棋」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例では、第１の非トラステッドＪａｖａ－ＡＰソフトウェアとする）に対応する説明ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２１１の内容は図１１に示される通りであり、移動機１６において解釈・実行されると図１２に示される説明ページ２１２を提供するように記述されている。また、ＡＤＦ２１３はパッケージＵＲＬとしてＪａｒファイル２１４のＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）を内包している。

【００７２】

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「星占い」なる名称のＪａｖａ－ＡＰソフトウェア（これを、本動作例では、第２の非トラステッド

ＪａｖａーＡＰソフトウェアとする）に対応する説明ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２０７の内容は図１３に示される通りであり、移動機１６において解釈・実行されると図１４に示される説明ページ２０８を提供するように記述されている。また、ＡＤＦ２０９はパッケージＵＲＬとしてＪａｒファイル２１０のＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

なお、上述した第１の非トラステッドＪａｖａーＡＰソフトウェアと第２の非トラステッドＪａｖａーＡＰソフトウェアの違いは、後者に関連する情報がリストファイル２００に登録されているのに対し、前者に関連する情報が登録されていない点にある。

【００７３】

また、ＩＰサーバ装置１３の不揮発性メモリ１３Ａには、「電話帳ビューア」なる名称のＪａｖａーＡＰソフトウェア（これを、本動作例ではトラステッドＪａｖａーＡＰソフトウェアとする）に対応する説明ファイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰによって作成されている。これらのうち、説明ファイル２０２の内容は図１５に示される通りであり、移動機１６において解釈・実行されると図１６に示される説明ページ２０３を提供するように記述されている。ＡＤＦ２０５は、ＡＰＩＤとして“0001”、ハッシュ値としてＪａｒファイル２０６のハッシュ値、パッケージＵＲＬとしてＪａｒファイル２０６のＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）、ＳＤＦーＵＲＬとしてＳＤＦ２０４のＵＲＬ（“http://www.aaa.co.jp/viewer.sdf”）、及び通信事業者の公開鍵を内包している。また、移動機１６は上述の各ＪａｖａーＡＰソフトウェアをインストール可能な状態にあるものとする。

【００７４】

（２－１）インストール動作

まず、ＪａｖａーＡＰソフトウェアを移動機１６にインストールする場合の動作例について、上述したＪａｖａーＡＰソフトウェア毎に説明する。

（２－１－１）第１の非トラステッドＪａｖａ－ＡＰソフトウェア

第１の非トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２１１の取得を試みることから始まる。これにより、移動機１６では、説明ファイル２１１のＵＲＬ（“http://www.ccc.co.jp/mno.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ１２が生成される。この要求メッセージｔｍ１２は、図１７に示されるように、移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１２の内容に対応して説明ファイル２１１を内包した応答メッセージｔｍ１３が生成される。この応答メッセージｔｍ１３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２１１の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１２に示すような説明ページ２１２が表示される。

【００７５】

この説明ページ２１２を視たユーザが、説明ページ２１２内のアンカー２１２Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１１の説明ファイル２１１に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/shogi.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２１３の送信を要求する内容の要求メッセージｔｍ１６が生成される。この要求メッセージｔｍ１６は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１６の内容に対応してＡＤＦ２１３を内包した応答メッセージｔｍ１７が生成される。この応答メッセージｔｍ１７はＩＰサーバ装置１２から送信され移動機１６により受信される。

【００７６】

移動機１６では、ＡＤＦ２１３の内容に基づいて第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、

移動機１６は非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００７７】

次に、移動機１６では、ＡＤＦ２１３が不揮発性メモリ１６Ｄに書き込まれる。また、移動機１６では、ＡＤＦ２１３からパッケージＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１４の送信を要求する内容の要求メッセージｔｍ１８が生成される。この要求メッセージｔｍ１８は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ１８の内容に対応してＪａｒファイル２１４を内包した応答メッセージｔｍ１９が生成される。この応答メッセージｔｍ１９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１４が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、第１の非トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において第１の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態はＡＤＦ２１３の取得を開始する前の状態に戻る。

【００７８】

（２－１－２）第２の非トラステッドＪａｖａ－ＡＰソフトウェアの

第２の非トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０７またはリストファイル２００の取得を試みることから始まる。説明ファイル２０７の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル２００の取得を試みることから始まる動作のみについて説明する。

【００７９】

図１８に示されるように、移動機１６では、リストファイル２００のＵＲＬ（

“http://www.aaa.co.jp/def.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２０が生成される。この要求メッセージｔｍ２０は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ２０の内容に対応してリストファイル２００を内包した応答メッセージｔｍ２１が生成される。この応答メッセージｔｍ２１は管理サーバ装置１８から送信され移動機１６により受信される。移動機１６では、応答メッセージｔｍ２１の受信を契機として、応答メッセージｔｍ２１内のリストファイル２００がＨＴＭＬに従って解釈され、移動機１６のユーザに対して、リストファイル２００の内容に応じたＵＩが提供される。この結果、移動機１６の表示部１６Ｃには、例えば図１０に示すようなリストページ２０１が表示される。

【００８０】

このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ｂが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ｂに対応付けられているＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２２が生成される。この要求メッセージｔｍ２２は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２２の内容に対応して説明ファイル２０７を内包した応答メッセージｔｍ２３が生成される。この応答メッセージｔｍ２３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０７の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１４に示すような説明ページ２０８が表示される。

【００８１】

この説明ページ２０８を視たユーザが、説明ページ２０８内のアンカー２０８Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１３の説明ファイル２０７に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT

”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/horoscope.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２０９の送信を要求する内容の要求メッセージｔｍ２６が生成される。この要求メッセージｔｍ２６は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２６の内容に対応してＡＤＦ２０９を内包した応答メッセージｔｍ２７が生成される。この応答メッセージｔｍ２７はＩＰサーバ装置１２から送信され移動機１６により受信される。

【００８２】

移動機１６では、ＡＤＦ２０９の内容に基づいて第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００８３】

次に、移動機１６では、ＡＤＦ２０９が不揮発性メモリ１６Ｄに書き込まれる。また、移動機１６では、ＡＤＦ２０９からパッケージＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１０の送信を要求する内容の要求メッセージｔｍ２８が生成される。この要求メッセージｔｍ２８は移動機１６から送信されＩＰサーバ装置１２により受信される。

ＩＰサーバ装置１２では、この要求メッセージｔｍ２８の内容に対応してＪａｒファイル２１０を内包した応答メッセージｔｍ２９が生成される。この応答メッセージｔｍ２９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１０が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、第２の非トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において、第２の非トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ

２０９の取得を開始する前の状態に戻る。

【００８４】

（２－１－３）トラステッドＪａｖａ－ＡＰソフトウェア

トラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０２またはリストファイル２００の取得を試みることから始まる。説明ファイル２０２の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル２０２の取得を試みることから始まる動作についての説明を省略する。

【００８５】

図１９に示されるように、リストファイル２００の取得を試みることから始まる動作において、移動機１６が応答メッセージｔｍ２１を受信し、例えば図１０に示すようなリストページ２０１が表示されるまでは図１８に示す動作と同一の動作が行われる。このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ａが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ａに対応付けられているＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ３２が生成される。この要求メッセージｔｍ３２は移動機１６から送信されＩＰサーバ装置１３により受信される。

ＩＰサーバ装置１３では、この要求メッセージｔｍ３２の内容に対応して説明ファイル２０２を内包した応答メッセージｔｍ３３が生成される。この応答メッセージｔｍ３３はＩＰサーバ装置１３から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０２の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１６に示すような説明ページ２０３が表示される。

【００８６】

この説明ページ２０３を視たユーザが、説明ページ２０３内のアンカー２０３Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１５の説明ファイル２０２に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性

に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.main.bbb.co.jp/viewer.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２０５の送信を要求する内容の要求メッセージｔｍ３４が生成される。この要求メッセージｔｍ３４は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３４の内容に対応してＡＤＦ２０５を内包した応答メッセージｔｍ３５が生成される。この応答メッセージｔｍ３５はＩＰサーバ装置１３から送信され、ゲートウェイサーバ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。

【００８７】

移動機１６において、ＡＤＦ２０５は不揮発性メモリ１６Ｄに書き込まれ、ＡＤＦ２０５の内容に基づいてトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６はトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６ではトラステッドＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００８８】

そして、移動機１６では、ＡＤＦ２０５に内包されているＳＤＦ－ＵＲＬ“http://www.aaa.co.jp/viewer.sdf”で特定されるＳＤＦ２０４の送信を要求する内容の要求メッセージｔｍ３６が生成される。この要求メッセージｔｍ３６は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ３６の内容に対応してＳＤＦ２０４を内包した応答メッセージｔｍ３７が生成される。この応答メッセージｔｍ３７は管理サーバ装置１８から送信されゲートウェイ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。ここで、管理サーバ装置１８とゲートウェイサーバ装置１７との間の通信路は専用線であり、ゲートウェイサーバ装置１７はセキュリティの確保された移動パケット通信網１５に直接的に接続されていることから、移動機１６に受信されるまでにＳＤＦ２０４が改竄される虞は無い。

【００８９】

さらに、移動機１６では、ＡＤＦ２０５に内包されている公開鍵を用いてＳＤＦ２０４の正当性が判断される。前述のように、ＡＤＦ２０５に内包されている公開鍵はＳＤＦ２０４への署名の際に用いた秘密鍵と対応していることから、管理サーバ装置１８内においてＳＤＦ２０４の内容が変更されていない限り、ＳＤＦ２０４が正当であると判断される。

【００９０】

ＳＤＦ２０４が正当であると判断されると、移動機１６では、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡＰＩＤとが比較される。前述のように、ＩＰサーバ装置１３におけるＡＤＦ２０５にはＳＤＦ２０４内のＡＰＩＤと一致するＡＰＩＤが記述されるように定められていることから、記述ミス等が無い限り、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡＰＩＤは一致する。次いで、移動機１６では、ＳＤＦ２０４が不揮発性メモリ１６Ｄに書き込まれる。

【００９１】

次に、移動機１６では、ＡＤＦ２０５からパッケージＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２０６の送信を要求する内容の要求メッセージｔｍ３８が生成される。この要求メッセージｔｍ３８は移動機１６から送信されＩＰサーバ装置１３により受信される。

ＩＰサーバ装置１３では、この要求メッセージｔｍ３８の内容に対応してＪａｒファイル２０６を内包した応答メッセージｔｍ３９が生成される。この応答メッセージｔｍ３９はＩＰサーバ装置１３から送信され移動機１６により受信される。

【００９２】

次に、移動機１６ではＪａｒファイル２０６と所定のハッシュ関数とを用いてハッシュ値が算出され、このハッシュ値とＡＤＦ２０５に内包されているハッシュ値とが比較される。前述のように、ＡＤＦ２０５にはこのＡＤＦ２０５に対応するＪａｒファイルのハッシュ値が記述されるように定められていることから、

記述ミス等がない限り、両ハッシュ値は一致する。

両ハッシュ値が一致すると、移動機１６では、Ｊａｒファイル２０６が不揮発性メモリ１６Ｄに起動可能な状態で書き込まれ、これにより、トラステッドＪａｖａ－ＡＰソフトウェアのインストールが完了する。

【００９３】

なお、移動機１６においてＳＤＦ２０４が正当でないと判断された場合や、ＡＤＦ２０５に内包されているＡＰＩＤとＳＤＦ２０４に内包されているＡＰＩＤが不一致の場合、トラステッドＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とＡＤＦ２０５に内包されているハッシュ値とが不一致の場合には、移動機１６の状態はＡＤＦ２０５の取得を開始する前の状態に戻る。

【００９４】

（２－２）Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動

次に、上述の各々のＪａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動について説明する。

（２－２－１）非トラステッドＪａｖａ－ＡＰソフトウェアの挙動

上述したインストール動作により移動機１６にインストールされた非トラステッドＪａｖａ－ＡＰソフトウェア（第１の非トラステッドＪａｖａ－ＡＰソフトウェア（詰め将棋）及び第２の非トラステッドＪａｖａ－ＡＰソフトウェア（星占い）の双方を含む）が、ＪＡＭが実現された移動機１６において起動され、このソフトウェアに対応した機能（以後、非トラステッドＪａｖａ－ＡＰ）が移動機１６内に実現されたときの移動機１６の挙動について説明する。

【００９５】

非トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合、前述したように非トラステッドＡＰＩはあらゆるＪａｖａ－ＡＰの使用が許可されているから、この場合のＡＰＩの使用はＪＡＭにより許可されることとなる。したがって、非トラステッドＪａｖａ－ＡＰはこの非トラステッドＡＰＩを使用することができる。

また、非トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッ

ドＡＰＩの場合、ＪＡＭはこのＪａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄに記憶されているか否かを調べる。ここでは、そのようなＳＤＦは不揮発性メモリ１６Ｄに記憶されていないから、ＪＡＭは非トラステッドＪａｖａ－ＡＰによるこのＡＰＩの使用を禁止する。したがって、非トラステッドＪａｖａ－ＡＰはトラステッドＡＰＩを使用することができない。

【００９６】

（２－２－２）トラステッドＪａｖａ－ＡＰソフトウェアの挙動

移動機１６にインストールされたトラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）が、ＪＡＭが実現された移動機１６において起動され、このソフトウェアに対応した機能が移動機１６内に実現されたときの移動機１６の挙動について説明する。

トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合、前述したように、このＡＰＩの使用はＪＡＭによって当然許可される。したがって、トラステッドＪａｖａ－ＡＰはこの非トラステッドＡＰＩを使用することができる。

トラステッドＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、このＪａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄに記憶されているので、このＡＰＩの使用はＪＡＭによって許可され得るが、そのトラステッドＪａｖａ－ＡＰの挙動はＳＤＦ内のポリシー情報に依存する。以下、使用するＡＰＩ毎にその挙動について説明する。

【００９７】

（２－２－２－１）getPhoneList()

“getPhoneList()”はトラステッドＡＰＩであるから、このＡＰＩの使用の可否は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図４に示される通りであることから、“getPhoneList()”の使用がＪＡＭにより許可される。したがって、トラステッドＪａｖａ－ＡＰ（電話帳ビューワ）は“getPhoneList()”を使用することができる。つまり、このトラステッドＪａｖａ－ＡＰは電話帳データを読み出すことができる。

【００９８】

（２－２－２－２）getCallHistory()

“getCallHistory()”はトラステッドＡＰＩであるから、このＡＰＩの使用の可否はＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図４に示される通りであることから、“getCallHistory()”の使用がＪＡＭにより禁止される。したがって、トラステッドＪａｖａ－ＡＰ（電話帳ビューワ）は“getCallHistory()”を使用することができない。つまり、このトラステッドＪａｖａ－ＡＰは発着信履歴データを読み出すことができない。

【００９９】

（２－３）トラステッドＪａｖａ－ＡＰソフトウェアの有効期限更新時の動作

次に、トラステッドＪａｖａ－ＡＰソフトウェアの有効期限を更新する動作例について説明する。以下の説明においては、図９において、管理サーバ装置１８内においてＳＤＦ２０４がＳＤＦ２０４ａに更新されているものとする。ただし、その更新内容は、有効期限が“２００２年１０月１日午前１０時”から“２００３年１月１日午前１０時”に変更されたということのみであり、ＳＤＦ２０４とＳＤＦ２０４ａの記憶位置やそのファイル名、署名に用いた秘密鍵等は一切変更されていないものとする。

【０１００】

移動機１６は、計時部１６Ｈによって計時される現在日時と、今までに取得した全てのＳＤＦに内包されている複数の有効期限とを常時監視しており、有効期限が到来したか否かを判断している。ここで、計時部１６Ｈによって計時される現在日時が２００２年１０月１日午前１０時となったとき、ＡＰＩＤ“0001”に対応するトラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）の有効期限が到来することとなり、これによって、図２０に示す動作が開始される

【０１０１】

まず、移動機１６は、図２１に示すように、有効期限が到来したトラステッドＪａｖａ－ＡＰソフトウェアの名称“電話帳ビューワ”とともに、有効期限が到来したので更新するか否かをユーザに問い合わせるメッセージを表示部１６ｃに

表示してユーザの操作があるまで待機する。

ここで、ユーザが有効期限を更新することを指示する操作を行うと、移動機１６はこの指示内容を解釈し、ＡＰＩＤ“0001”を内包したＡＤＦに内包されているＳＤＦ－ＵＲＬ（“http://www.aaa.co.jp/viewer.sdf”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ４１を生成する。この要求メッセージｔｍ４１は移動機１６から送信され管理サーバ装置１８により受信される。

管理サーバ装置１８では、この要求メッセージｔｍ４１の内容に対応してＳＤＦ２０４ａを内包した応答メッセージｔｍ４２が生成される。この応答メッセージｔｍ４２は管理サーバ装置１８から送信され移動機１６により受信される。

【０１０２】

一方、移動機１６は、上記ＳＤＦ－ＵＲＬを用いてＳＤＦ２０４ａを取得できたか否かを判断する。ここでは取得に成功することを想定しているので処理は次に進み、移動機１６は、ＳＤＦ２０４ａの署名を、既に取得しているＡＤＦ２０５に内包されている公開鍵を用いて検証し（復号し）、このＳＤＦ２０４ａの正当性を判断する。正当性が確認されると（ステップＳ３５；Ｙｅｓ）、移動機１６は、ＳＤＦ２０４ａから抽出したＡＰＩＤと既に取得済みのＡＤＦ２０５に内包されていたＡＰＩＤとを比較し、両者が一致するか否かを判定する。

ここでは両者が一致するはずなので、移動機１６は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０３をＳＤＦ２０４ａで上書きし、これにより、トラステッドＪａｖａ－ＡＰソフトウェア（電話帳ビューワ）の有効期限が“２００２年１０月１日午前１０時”から“２００３年１月１日午前１０時”に更新される。

なお、ユーザの操作により有効期限を更新しないと判断された場合、ＳＤＦを取得できなかった場合、ＳＤＦが正当でないと判断した場合、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合、ＪＡＭは、有効期限を更新しない旨をユーザに通知するとともに、移動機１６の状態をＳＤＦ２０３ａを取得する以前の状態に戻す。

【０１０３】

（２－４）トラステッドＪａｖａ－ＡＰソフトウェアの変更後の動作

次に、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰがトラステッドＪａｖａ－ＡＰソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、トラステッドＪａｖａ－ＡＰソフトウェアの改善等を目的としたＪａｒファイル２０６の内容の変更と、ＩＰサーバ装置１３の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰは、図２２に示すように、変更後のＪａｒファイル２０６（以後、Ｊａｒファイル２１５）をＩＰサーバ装置１４の不揮発性メモリ１４Ａに記憶させ、このＪａｒファイル２１５に対応するようにＡＤＦ２０５の内容を変更してＡＤＦ２１６としている。変更後のトラステッドＪａｖａ－ＡＰソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置１８を管理する通信事業者が行うべき作業は存在しない。つまり、通信事業者はリストファイル２００やＳＤＦ２０４を変更する必要はない。

【０１０４】

このような変更の後のトラステッドＪａｖａ－ＡＰソフトウェアのインストール動作は、図２３に示す通りとなる。この図に示す動作が図１９に示す動作と相違し始めるのは、移動機１６がＪａｒファイルを要求する時点からである。なお、両図において、応答メッセージｔｍ４７は応答メッセージｔｍ３７、要求メッセージｔｍ４８は要求メッセージｔｍ３８、応答メッセージｔｍ４９は応答メッセージｔｍ３９に対応している。

即ち、図２３において図１９に示す動作と本質的に異なるのは、ＡＤＦ２１６およびＪａｒファイル２１５が処理の対象となる点と、ＡＤＦ２１６に内包されているパッケージＵＲＬ（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるＪａｒファイル２１５の送信を要求する内容の要求メッセージｔｍ４８が移動機１６にて生成される点と、この要求メッセージｔｍ４８が移動機１６から送信されＩＰサーバ装置１４により受信される点と、ＩＰサーバ装置１４においてＪａｒファイル２１５を内包した応答メッセージｔｍ４９が生成される点と、この応答メッセージｔｍ４９がＩＰサーバ装置１４から送信され移動機１６により受信される点のみである。

【０１０５】

以上説明したように、移動機１６においては、ダウンロードしたＳＤＦに含まれるポリシー情報の内容に応じた挙動がこのＳＤＦに対応するトラステッドＪａｖａ－ＡＰソフトウェアに許可され、ポリシー情報の内容に含まれていない挙動は許可されない。このポリシー情報は管理サーバ装置１８からセキュリティが確保された上で移動機１６へ送信されるから、ポリシー情報が第三者により改竄される虞もなく、これにより、トラステッドＪａｖａ－ＡＰの信頼性が確保される。また、ユーザから視れば、従来通りの非トラステッドＪａｖａ－ＡＰの他に、上記のような、より自由な挙動が許可されたトラステッドＪａｖａ－ＡＰを利用可能となり、非常に便利である。

【０１０６】

なお、上述の配信システムにおいては、移動機１６に対し、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各種ファイルの配信を行っていたが、このような順序で配信することにより、以下のような効果が生ずる。

既に説明したように、Ｊａｖａ－ＡＰソフトウェア（ＡＤＦ及びＪａｒファイル）はＩＰによって設計・作成され、各々のＩＰがインターネット上に開設している専用サイト（図１のＩＰサーバ装置１２～１４）において、一般ユーザに公開されている。従って、ユーザはまず、ＩＰの専用サイトにアクセスし、そこで、様々なＪａｖａ－ＡＰソフトウェアの解説ページを参照してそのソフトウェアをダウンロードをするか否かを判断するのが普通である。そして、ユーザはＪａｖａ－ＡＰソフトウェアをダウンロードしようと判断すると、そのダウンロード処理を指示する操作を行う必要があるが、そのために上記の解説ページには次にダウンロードすべきファイルのＵＲＬがアンカータグによって埋め込まれているのが普通である。このとき、ＩＰの立場から視れば、解説ページにＡＤＦのＵＲＬを埋め込むのが最も手間がかからない。なぜなら、ＡＤＦはＩＰの管理下にあるので、そのＡＤＦのＵＲＬはＩＰによって常に把握できているからである。これに対し、解説ページにＳＤＦのＵＲＬを埋め込むとなると、ＩＰは通信事業者に問い合わせをする等して、ＵＲＬの正誤の確認処理を絶えず欠かさないようにしなければならない。よって、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各

種ファイルの配信を行うことは非常に有意義である。

【０１０７】

また、上記の順序は、エヌティティドコモ社のｉモード（登録商標）において現在実施されているＪａｖａ－ＡＰソフトウェアのバージョンアップ処理を考慮した場合にも利点がある。現状のｉモードのサービス仕様においては、ユーザによってバージョンアップを要求する操作がなされると、移動機は、まず、ＡＤＦに記述された内容を参照し、ＡＤＦに記述されたパッケージＵＲＬに基づいて、バージョンアップ後のＪａｒファイルを取得するようになっている。即ち、バージョンアップ時には、まずＡＤＦを参照してから、その後にダウンロード処理に移行するようになっている。この点を考慮すると、本実施形態の配信システムにおけるバージョンアップ時においても、まずＡＤＦを参照し、そのＡＤＦに記述されているＳＤＦ－ＵＲＬに基づいてＳＤＦを取得した後、Ｊａｒファイルを取得するというように、まずＡＤＦの参照から一連の処理を開始すると、それ以降は、ＳＤＦ→Ｊａｒファイルという通常のダウンロードと同じ流れで処理を行うことができ、現状のサービス仕様をあまり変更しないで済む。これに対し、仮にＳＤＦ、ＡＤＦ、Ｊａｒファイルという順序で各種ファイルをダウンロードすることが定義付けられている場合、バージョンアップしようとした場合、ＡＤＦを参照からダウンロード処理を開始すると、ＳＤＦを取得することなくＪａｒファイルの取得処理にまで至ってしまう。ＳＤＦは、バージョンアップ時に書き換えられることは十分にあり得るので、ＳＤＦが無いとセキュリティ上で不都合が生ずるおそれがある。以上のような観点からも、ＡＤＦ、ＳＤＦ、Ｊａｒファイルという順序で各種ファイルの配信を行うことは有意義である。

【０１０８】

（３）変形例

本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてＳＤＦとＡＤＦの作成者との対応関係の正当性を確認するようにした。しかし、これに限らず、ＳＤＦとＡＤＦの作成者との対応関係の正当性が確認でき

る方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、ＳＤＦに公開鍵を内包させず、ＩＰサーバ装置においてはＡＤＦに対する秘密鍵を用いた署名を行わず、かつ移動機においてはこの確認処理を省略する、という形態とし、移動機およびＩＰサーバ装置における処理量や、移動機と管理サーバ装置およびＩＰサーバ装置との間の通信量を低減するようにしてもよい。

【０１０９】

また、上述した配信システムでは、Ｊａｒファイルのハッシュ値をこのＪａｒファイルに対応するＡＤＦに内包させる一方、移動機においてＪａｒファイルのハッシュ値を生成し、これら両者を比較してＪａｒファイルとＡＤＦとの対応関係の正当性を確認するようにしていた。しかし、これに限らず、Ｊａｒファイルとの対応関係の正当性が確認できる方式であればどのような方式を用いてもよい。

また、システムに要求されるセキュリティレベルによっては、ＡＤＦにハッシュ値を内包させずにこの確認処理を省略する形態とし、移動機およびＩＰサーバ装置における処理量や移動機とＩＰサーバ装置との間の通信量を低減するようにしてもよい。

【０１１０】

また、上述した配信システムでは、トラステッドＪａｖａ－ＡＰに固有のＡＰＩＤを使用してＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドＪａｖａ－ＡＰを提供する情報提供事業者に固有のＣＩＤを用いてＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、ＡＰＩＤやＣＩＤを用いた判定を省略するようにしてもよい。

【０１１１】

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、ＩＰアドレスを用いてサーバを指定するようにしてもよい。

【０１１２】

また、移動機において、ＡＤＦに内包されているＳＤＦ－ＵＲＬのうちのドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、ＳＤＦを正当と認める態様としてもよい。この場合、予め設定された文字列と異なるときは、移動機１６は、ＳＤＦ取得に失敗した旨を表示し、管理サーバ１８にＳＤＦを要求せずに処理を終了することとなる。

また、この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のＲＯＭまたは不揮発性メモリに予め格納されることになる。ＲＯＭに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

【０１１３】

また、上述した配信システムでは、ＳＤＦの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がＳＤＦを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、ＳＤＦを暗号化した後に配信し、移動機においてＳＤＦを復号するようにすれば、ある程度のセキュリティを確保してＳＤＦを配信することができる。

【０１１４】

上述した配信システムでは、ＨＴＴＰに従ってファイルを送受するようにしたが、ＨＴＴＰＳを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

【０１１５】

また、上述した配信システムにおいて、信頼できる機関がＩＰとなってよいこと、すなわち、管理サーバ装置がＩＰサーバ装置を兼ねるようにしてもよいことは言うまでもない。

【０１１６】

さらに、上述した配信システムでは、Ｊａｖａ－ＡＰによる利用を制限する対象としてＡＰＩを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、ＬＥＤ（Light Emitting Diode）等の移動機が備え得るものや、移動機と共働し得るＵＩＭ（User Identity Module）やＳＩＭ（Subscriber Identity Module）等の外部機器なども挙げられる。

【０１１７】

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

【０１１８】

次にソフトウェア資源について説明する。ソフトウェア資源としては、ＡＰＩやクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Ｗｅｂブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

【０１１９】

ところで、Ｊａｖａ－ＡＰによるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限する

ことにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Ｊａｖａ－ＡＰのうちのトラステッドＪａｖａ－ＡＰについてのみ、自他のＪａｖａ－ＡＰの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

【０１２０】

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの２つの利用形態（利用の種類）があるから、非トラステッドＪａｖａ－ＡＰには読み出しでしか利用されないが、トラステッドＪａｖａ－ＡＰには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、１つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するＪａｖａ－ＡＰが起動されている間にＷｅｂブラウザ等が起動された場合、このＪａｖａ－ＡＰが「パケット伝送路の利用を排他的に行う」ことを許可されていないＪａｖａ－ＡＰであればＷｅｂブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているＪａｖａ－ＡＰであればパケット伝送路を占有して使用することができる、といった制御が可能となる。

さらに、この例を変形することで、ある種のパーミッションを与えられたＪａ

ｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはパケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

【０１２１】

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

【０１２２】

また、上述の配信システムでは、Ｊａｖａ－ＡＰの実行時にＪａｖａ－ＡＰの挙動を制限するようにしたが、ＩＰサーバ装置に格納されているＪａｒファイルにポリシー情報を内包させ、Ｊａｒファイルのダウンロード時に、移動機において、このポリシー情報とＳＤＦ中とのポリシー情報とを比較し、両者が一致しない場合には、このＪａｒファイルに対応するＪａｖａ－ＡＰを起動できないように、あるいはこのＪａｒファイルを含むＪａｖａ－ＡＰソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

【０１２３】

通信事業者の公開鍵は、ＩＰサーバ装置１２～１４からＡＤＦに含めて移動機１６に提供されるようになっていたが、これに限らず、予め移動機に格納されていてもよい。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、ＲＯＭに書き込んだ後に移動機を販売する

方法などが考えられる。

【０１２４】

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

【０１２５】

上述の配信システムでは、トラステッドＪａｖａ－ＡＰソフトウェアの有効期限が到来したタイミングで、その有効期限を更新するための処理を開始していた。しかし、更新タイミングは上記のものに限らず、ユーザが所望する恣意的なタイミングや、毎月末１回等の定期的なタイミングというように、様々な態様を採用し得る。

また、有効期限の設定の仕方は、既に説明したように日時によって設定してもよいが、この他にも、例えばトラステッドＪａｖａ－ＡＰソフトウェアのダウンロード時からの期間（例えばダウンロードしてから１ヶ月のみ使用可能というような場合）によって設定してもよいし、トラステッドＪａｖａ－ＡＰソフトウェアの実行回数や実行期間によって設定してもよい。要するに、有効期限とは、Ｊａｖａ－ＡＰソフトウェアを無制限には実行できないようにその上限を定めた情報であればどのようなものであってもよい。

例えば実行回数で有効期限を設定した場合、トラステッドＪａｖａ－ＡＰソフトウェアの起動時にＪＡＭはＳＤＦ内のポリシー情報を参照するようになっているので、その参照回数をトラステッドＪａｖａ－ＡＰソフトウェアの実行回数としてカウントしてもよい。そして、カウントした実行回数が予め定められた数に達すると、その更新処理に移行すればよい。

また、トラステッドＪａｖａ－ＡＰソフトウェアが実行されている期間を累積してカウントするような手段（例えばそのトラステッドＪａｖａ－ＡＰソフトウェア内にサブルーチンとして記述する等の手段）を備えていれば、実行期間によって有効期限を設定した場合にも対応できる。そして、カウントした実行期間が予め定められた時間に達すると、その更新処理に移行すればよい。

なお、上述の配信システムの説明では「トラステッドＪａｖａ－ＡＰソフトウェアの有効期限」という表現を用いていたが、より厳密には、Ｊａｒファイルそ

のものの有効期限であってもよいし、ＳＤＦそのものの有効期限であってもよいし、その両者の有効期限であってもよいことはもちろんである。

【０１２６】

また、上述の配信システムでは、有効期限が到来してもそれを更新できない場合、その有効期限が到来したトラステッドＪａｖａ－ＡＰソフトウェアを実行禁止となっていたが、これに限らず、その有効期限経過時にトラステッドＪａｖａ－ＡＰソフトウェアから非トラステッドＪａｖａ－ＡＰソフトウェアに遷移させてもよい。即ち、有効期限が到来したＪａｖａ－ＡＰソフトウェアは、非Ｊａｖａ－ＡＰソフトウェアであるとみなされ、その遷移後は、非トラステッドＪａｖａ－ＡＰソフトウェアとしての、より厳しい挙動を制限を受けることとなる。

【０１２７】

【発明の効果】

本発明によれば、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動がこのセキュリティ記述ファイルに対応するアプリケーションに許可される。したがって、多様なアプリケーションを提供することができる。さらに、権限を示す情報は管理サーバ装置からセキュリティが確保された上で端末装置へ送信されるから、権限が第三者により改竄される虞もなく、アプリケーションに対する信頼性が確保される。

【図面の簡単な説明】

【図１】　本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

【図２】　同システムに特有のＡＤＦのデータ構成を示す概念図である。

【図３】　同システムにおいて管理サーバ装置に格納されているＳＤＦのデータ構成を示す概念図である。

【図４】　同ＳＤＦに内包されるポリシー情報の内容を示す概念図である。

【図５】　同システムを構成する移動機の構成を示すブロック図である。

【図６】　同移動機の機能構成を示す概念図である。

【図７】　同移動機がＪａｖａ－ＡＰソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

【図８】　同移動機がＪａｖａ－ＡＰソフトウェアの有効期限を更新する処理の流れを示すフローチャートである。

【図９】　同配信システムの動作を説明するためのブロック図である。

【図１０】　同配信システムにて配信されるリストページを示す図である。

【図１１】　同配信システムを構成するＩＰサーバ装置が格納している説明ファイルの内容を示す図である。

【図１２】　同配信システムにて配信される説明ページを示す図である。

【図１３】　同ＩＰサーバ装置が格納している説明ファイルの内容を示す図である。

【図１４】　同配信システムにて配信される説明ページを示す図である。

【図１５】　同配信システムを構成するＩＰサーバ装置１３が格納し０ている説明ファイルの内容を示す図である。

【図１６】　同配信システムにて配信される説明ページを示す図である。

【図１７】　同配信システムの動作を説明するためのシーケンス図である。

【図１８】　同配信システムの動作を説明するためのシーケンス図である。

【図１９】　同配信システムの動作を説明するためのシーケンス図である。

【図２０】　同配信システムの動作を説明するためのシーケンス図である。

【図２１】　移動機にて表示される画面を示す図である。

【図２２】　同配信システムの他の動作を説明するためのブロック図である。

【図２３】　同配信システムの他の動作を説明するためのシーケンス図である。

【符号の説明】

１１	インターネット
１２、１３、１４	ＩＰサーバ装置
１５	移動パケット通信網
１６	移動機
１７	ゲートウェイサーバ装置
１８	管理サーバ装置

１６Ｄ、１２Ａ、１３Ａ、１４Ａ、１８Ａ　不揮発性メモリ

１６Ａ　　ＲＯＭ

１６Ｂ　　ＣＰＵ

１６Ｃ　　表示部

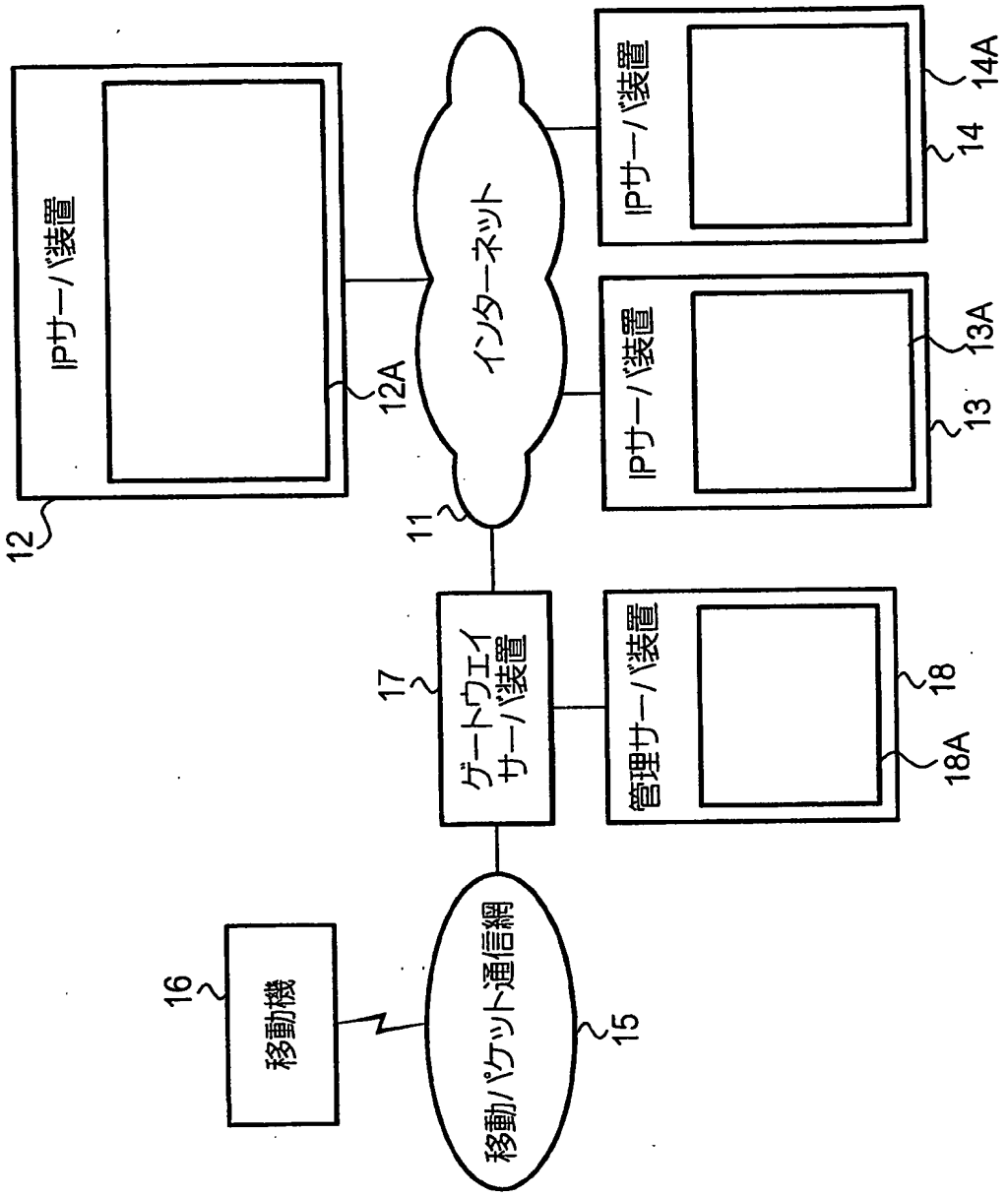
１６Ｅ　　ＲＡＭ

１６Ｆ　　通信部

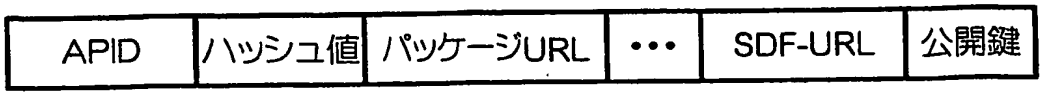
１６Ｇ　　操作部

【書類名】　　図面

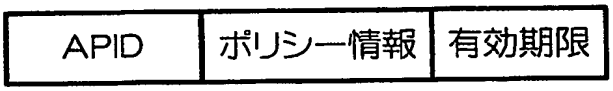
【図１】


IPサーバ装置
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
13
13A
ゲートウェイ
サーバ装置
17
管理サーバ装置
18
18A
移動パケット通信網
15
移動機
16

【図２】



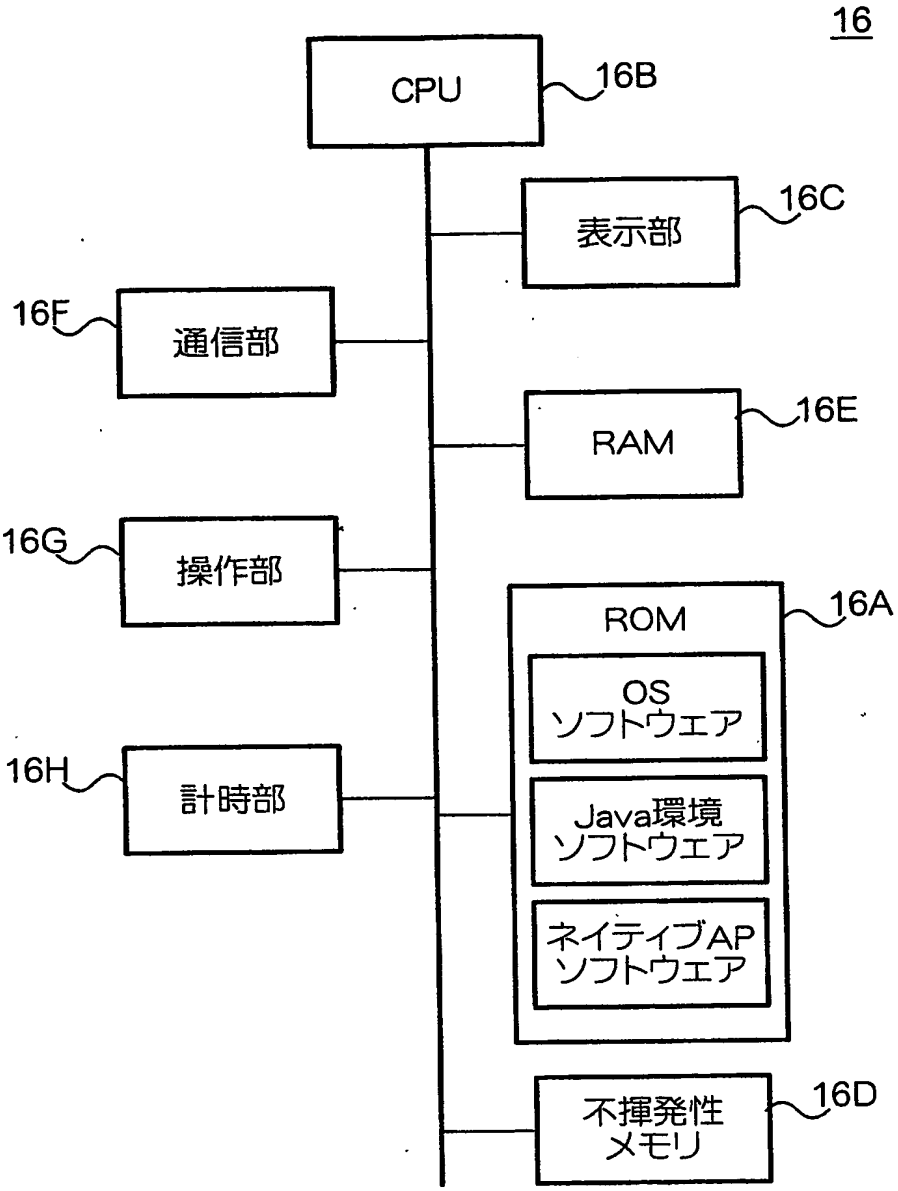
【図３】



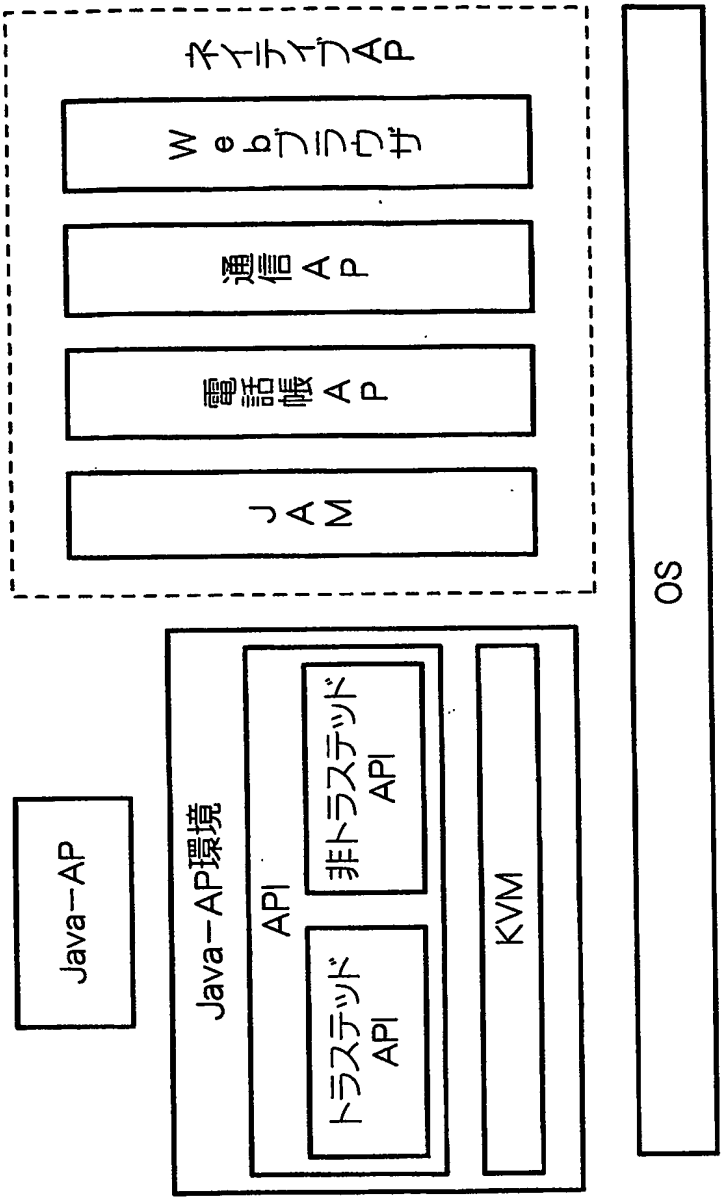
【図４】

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

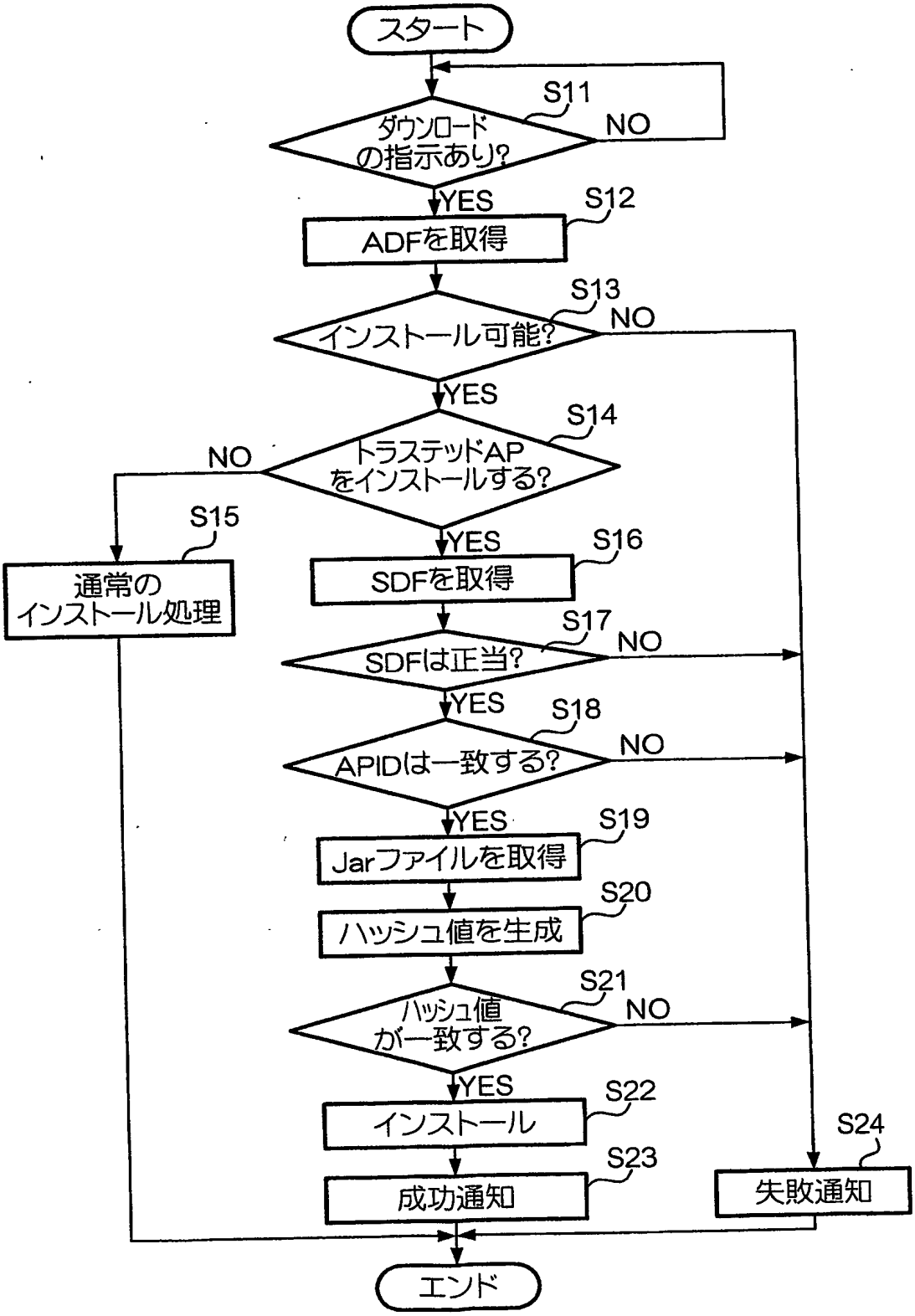
【図５】


16
CPU
16B
表示部
16C
16F
通信部
RAM
16E
16G
操作部
ROM
16A
OS
ソフトウェア
16H
計時部
Java環境
ソフトウェア
ネイティブAP
ソフトウェア
不揮発性
メモリ
16D

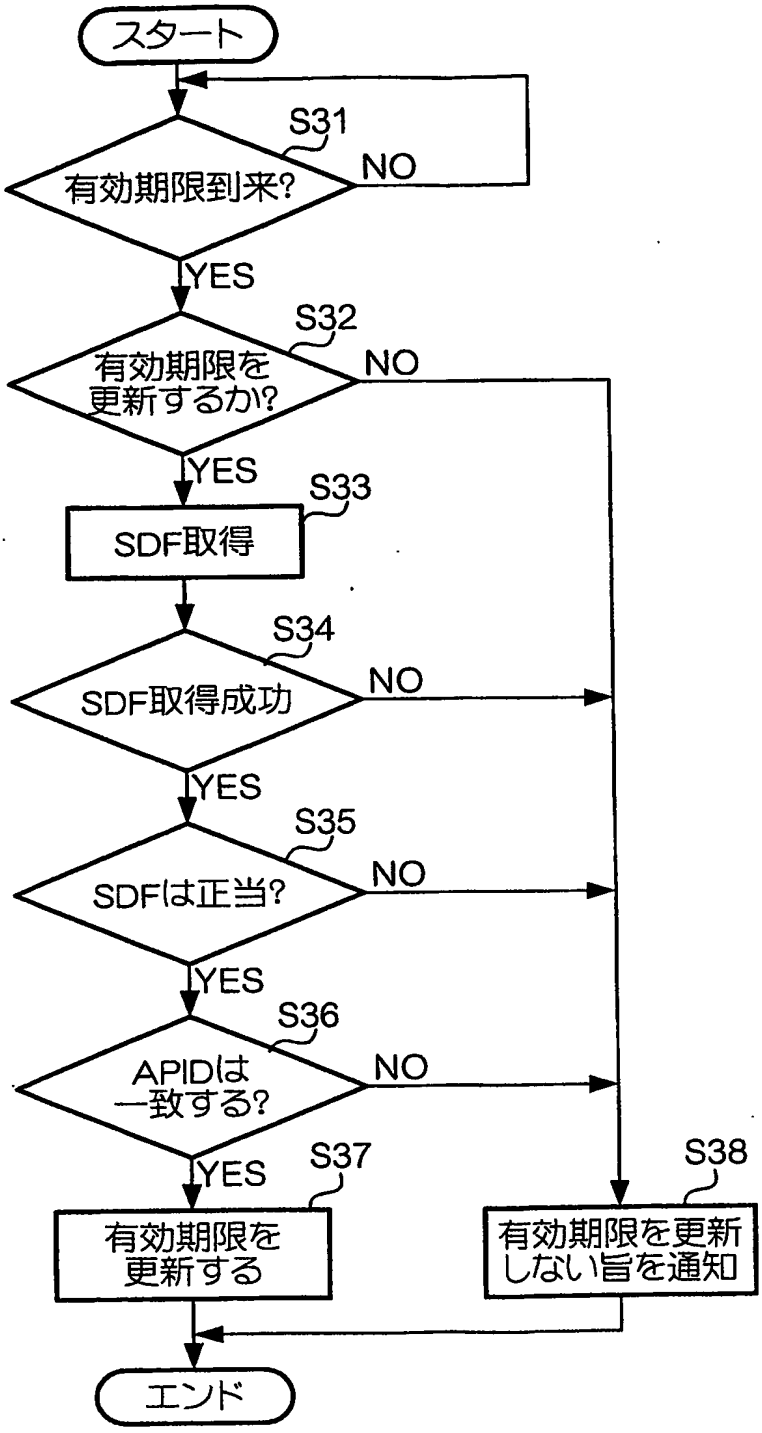
【図６】


ネイティブAP
Webブラウザ
通信AP
電話帳AP
JAM
OS
Java-AP
Java-AP環境
API
非トラステッドAPI
トラステッドAPI
KVM

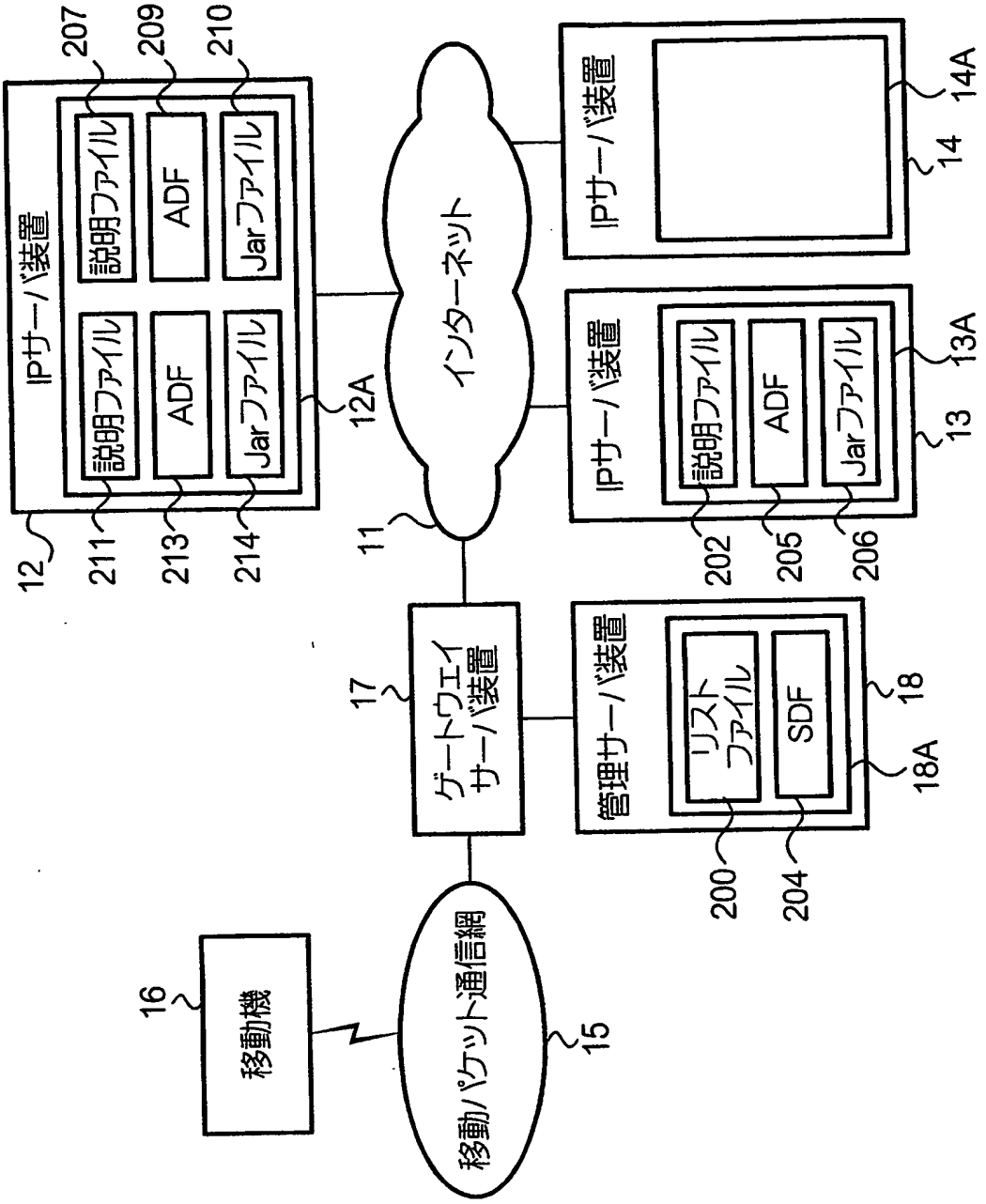
【図７】


スタート
S11
ダウンロードの指示あり?
NO
YES
S12
ADFを取得
S13
インストール可能?
NO
YES
S14
トラステッドAPをインストールする?
NO
YES
S15
通常のインストール処理
S16
SDFを取得
S17
SDFは正当?
NO
YES
S18
APIDは一致する?
NO
YES
S19
Jarファイルを取得
S20
ハッシュ値を生成
S21
ハッシュ値が一致する?
NO
YES
S22
インストール
S23
成功通知
S24
失敗通知
エンド

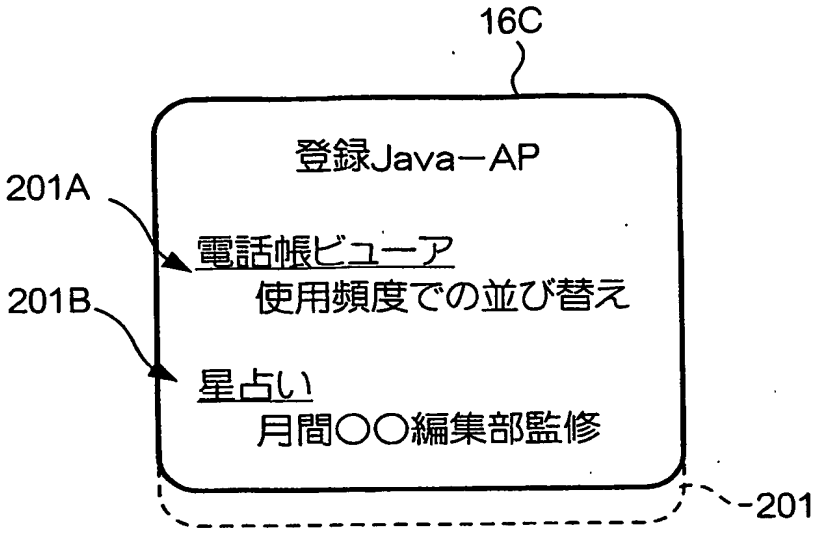
【図８】


スタート
S31
有効期限到来?
NO
YES
S32
有効期限を
更新するか?
NO
YES
S33
SDF取得
S34
SDF取得成功
NO
YES
S35
SDFは正当?
NO
YES
S36
APIDは
一致する?
NO
YES
S37
有効期限を
更新する
S38
有効期限を更新
しない旨を通知
エンド

【図９】


IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
説明ファイル
ADF
Jarファイル
13
13A
202
205
206
ゲートウェイサーバ装置
17
管理サーバ装置
リストファイル
SDF
18
18A
200
204
移動パケット通信網
15
移動機
16

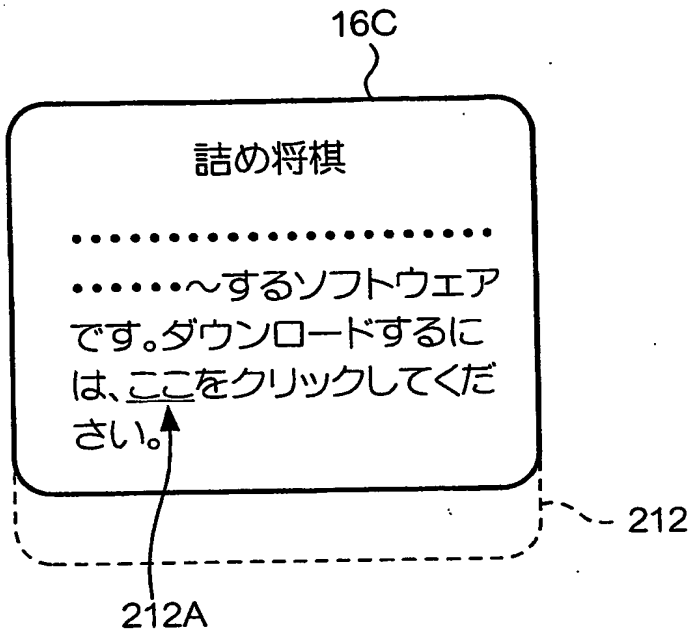
【図１０】



【図１１】

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/shogi.jam>
詰め将棋
</OBJECT>
～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。

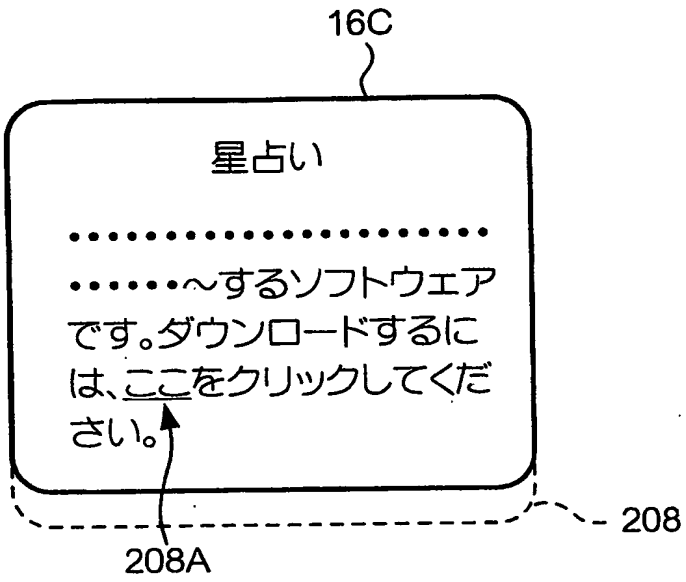
【図１２】



【図１３】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
星占い
</OBJECT>
   ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

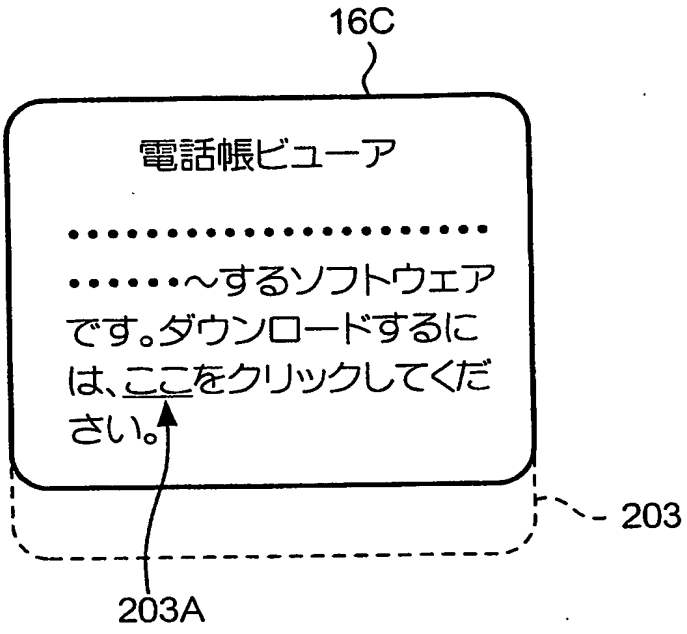
【図１４】



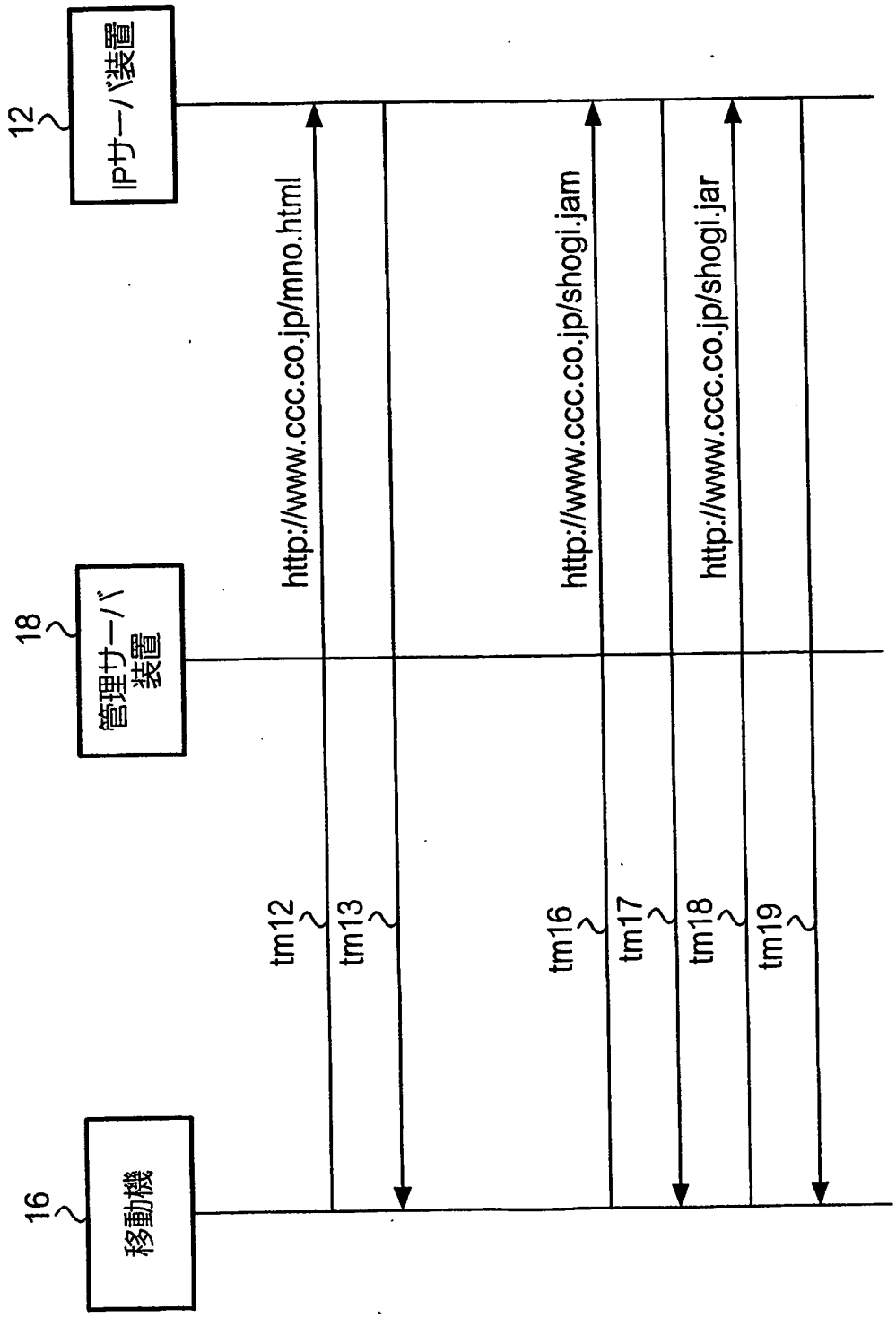
【図１５】

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/viewer.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
   ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

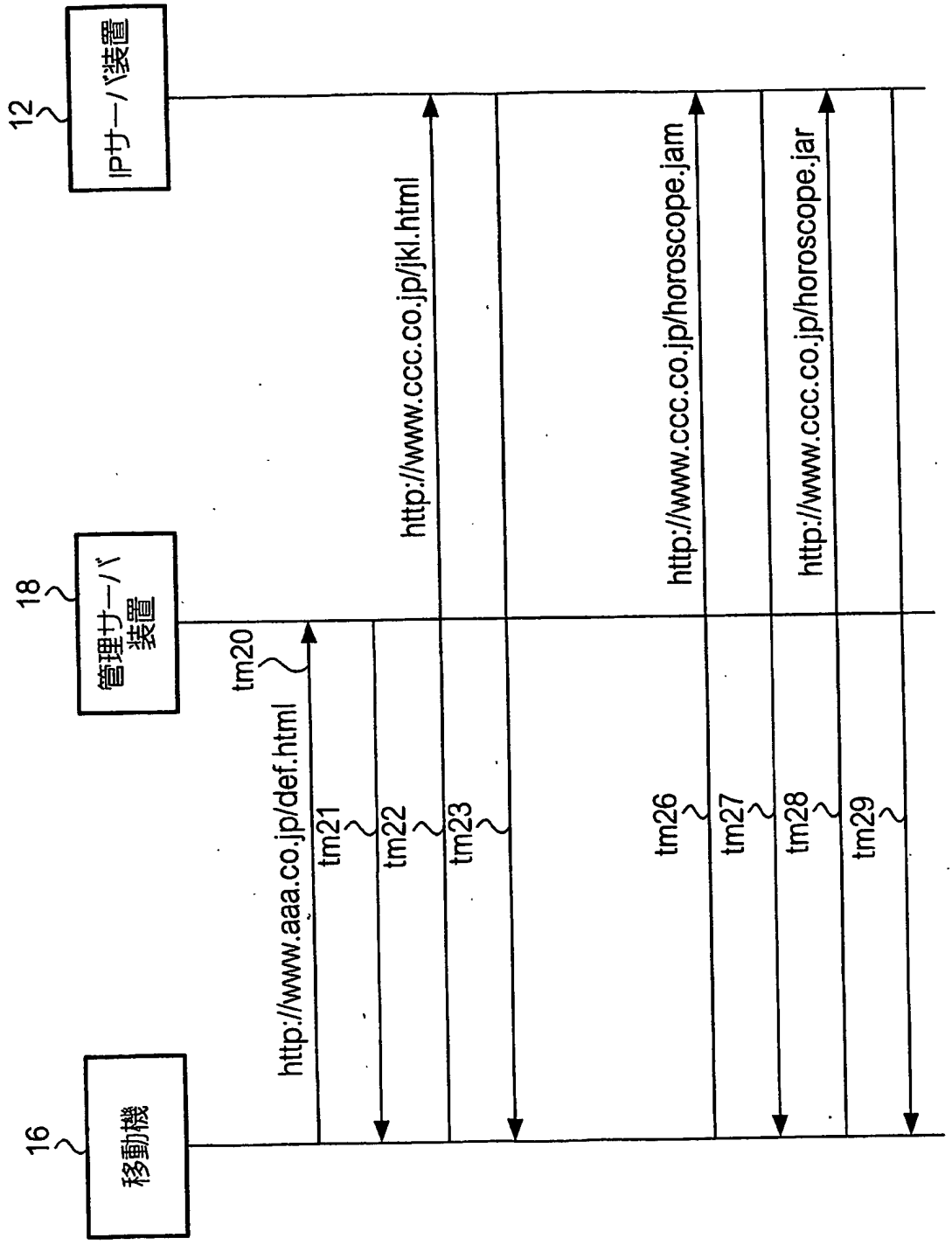
【図１６】


16C
電話帳ビューア
・・・・・・・・・・・・・・・・・・・・・・
・・・・・・～するソフトウェアです。ダウンロードするには、ここをクリックしてください。
203
203A

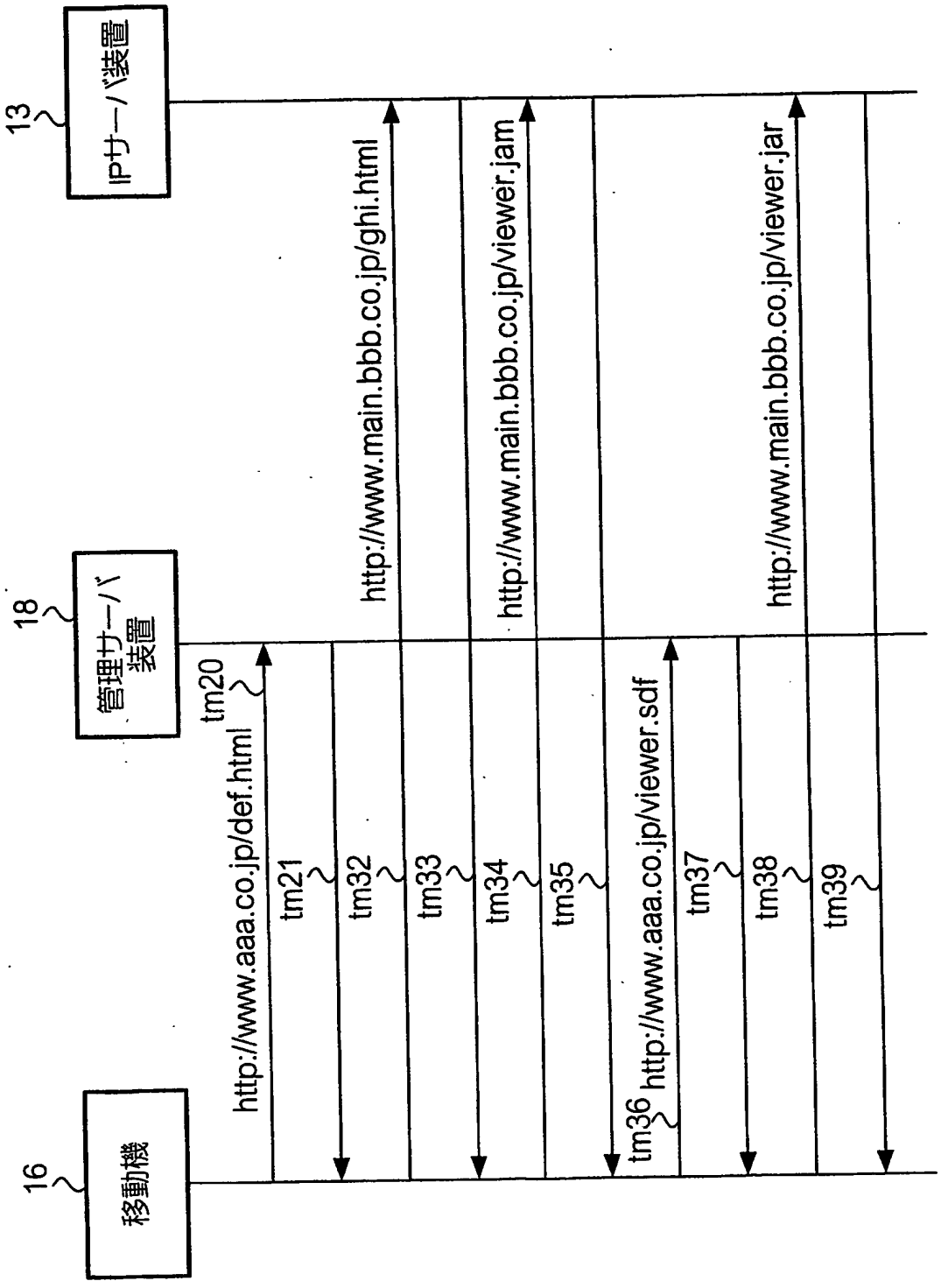
【図１７】


12
IPサーバ装置
18
管理サーバ装置
16
移動機
http://www.ccc.co.jp/mno.html
http://www.ccc.co.jp/shogi.jam
http://www.ccc.co.jp/shogi.jar
tm12
tm13
tm16
tm17
tm18
tm19

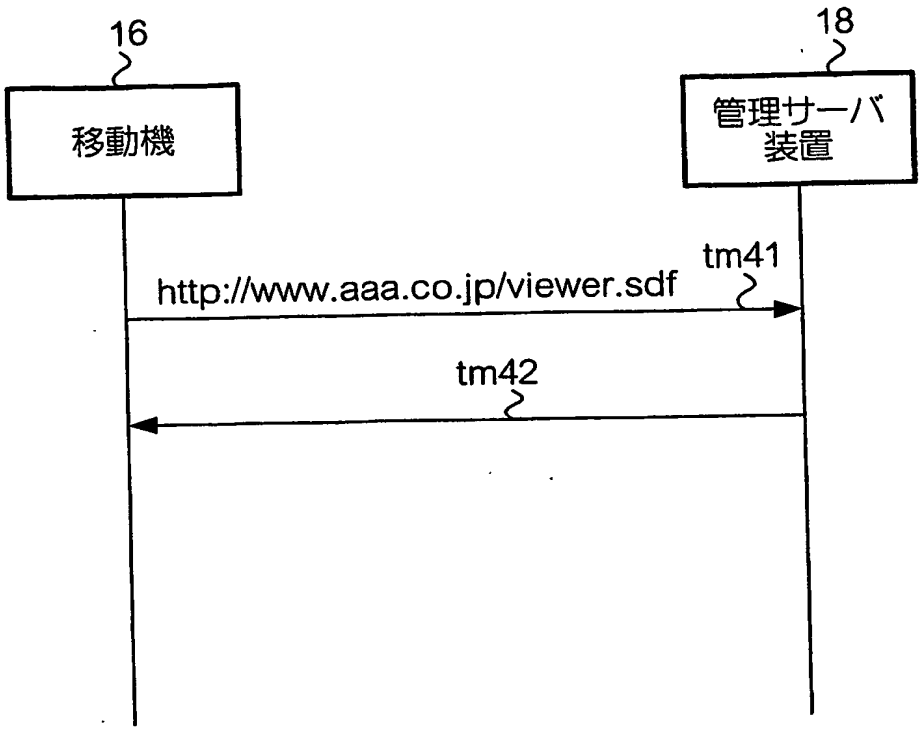
【図１８】


12
IPサーバ装置
18
管理サーバ装置
16
移動機
tm20
http://www.aaa.co.jp/def.html
tm21
tm22
tm23
http://www.ccc.co.jp/jkl.html
tm26
tm27
tm28
tm29
http://www.ccc.co.jp/horoscope.jam
http://www.ccc.co.jp/horoscope.jar

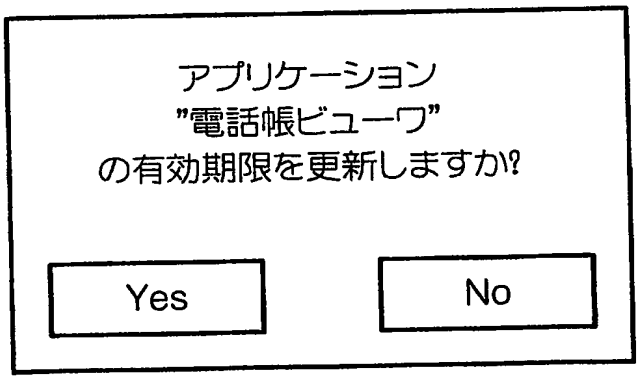
【図１９】


16
移動機
18
管理サーバ装置
13
IPサーバ装置
http://www.aaa.co.jp/def.html
tm20
tm21
tm32
http://www.main.bbb.co.jp/ghi.html
tm33
tm34
http://www.main.bbb.co.jp/viewer.jam
tm35
tm36
http://www.aaa.co.jp/viewer.sdf
tm37
tm38
http://www.main.bbb.co.jp/viewer.jar
tm39

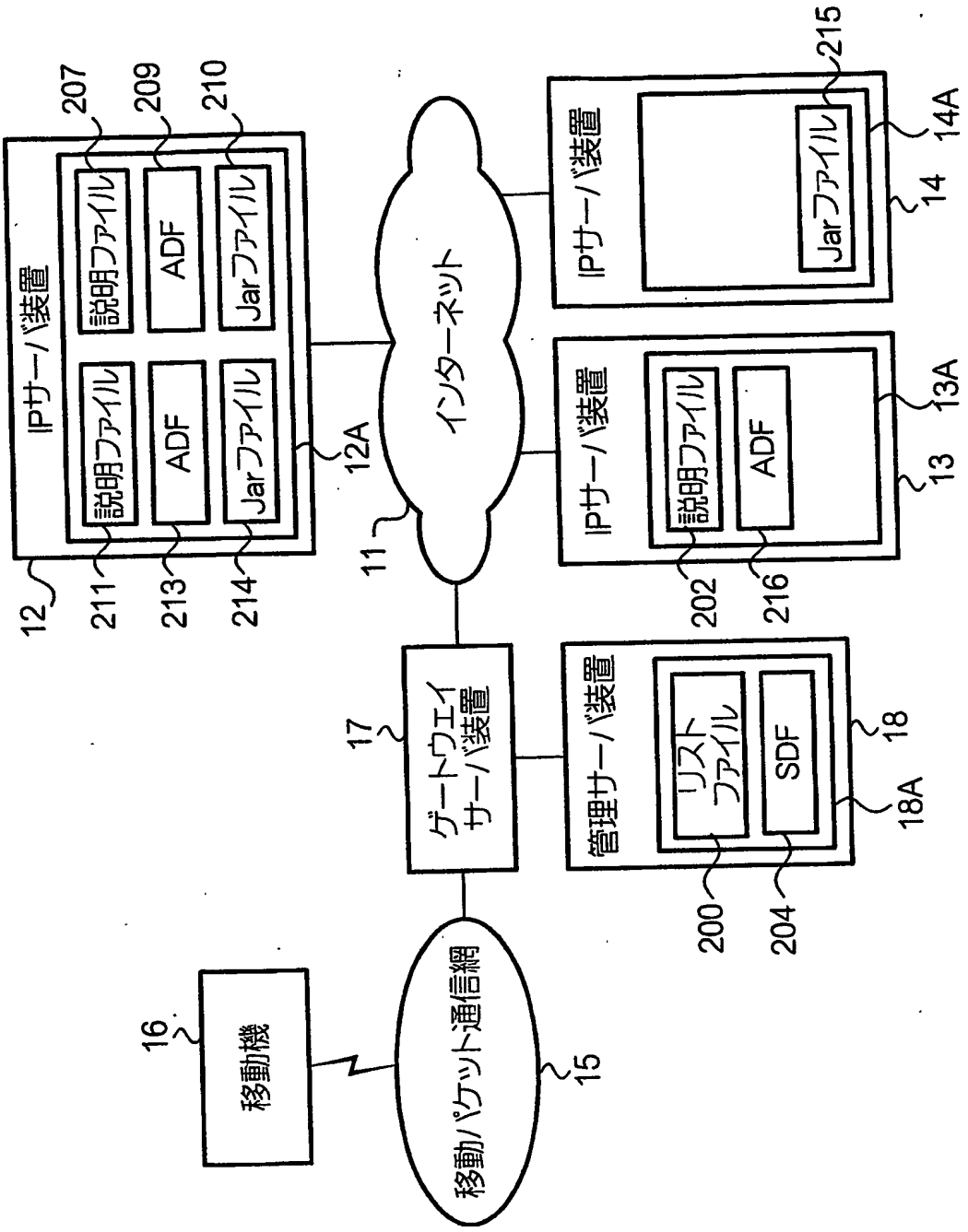
【図２０】


16
18
移動機
管理サーバ
装置
tm41
http://www.aaa.co.jp/viewer.sdf
tm42

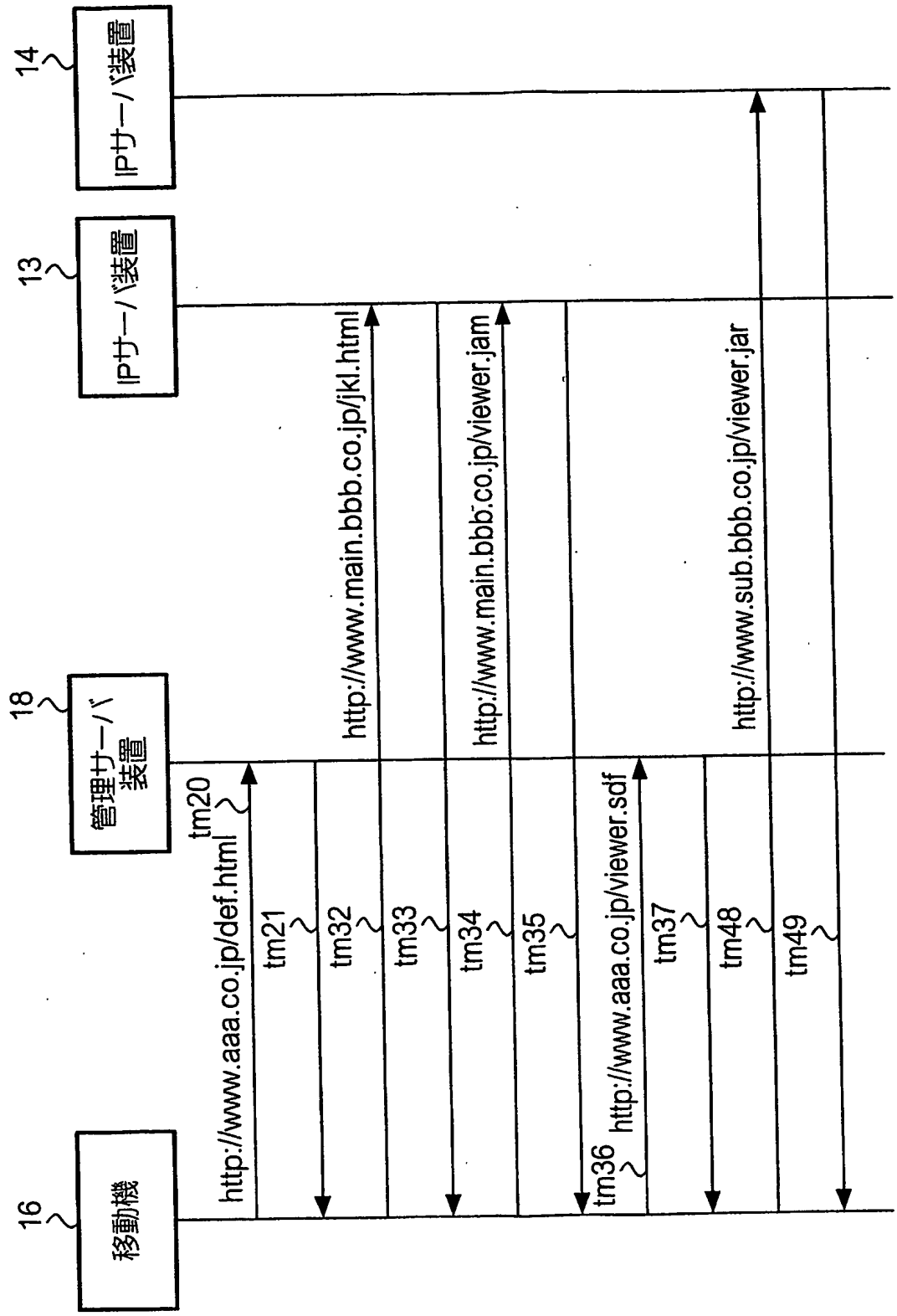
【図２１】


アプリケーション
"電話帳ビューワ"
の有効期限を更新しますか?
Yes
No

【図２２】


IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
Jarファイル
215
14
14A
IPサーバ装置
説明ファイル
ADF
202
216
13
13A
ゲートウエイサーバ装置
17
管理サーバ装置
リストファイル
SDF
200
204
18
18A
移動パケット通信網
15
移動機
16

【図２３】


16
移動機
18
管理サーバ装置
13
IPサーバ装置
14
IPサーバ装置
tm20
http://www.aaa.co.jp/def.html
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
http://www.main.bbb.co.jp/viewer.jam
tm35
tm36
http://www.aaa.co.jp/viewer.sdf
tm37
tm48
http://www.sub.bbb.co.jp/viewer.jar
tm49

【書類名】　　要約書

【要約】

【課題】　ＩＰの自由度を制限することなく、信頼性の保証されたＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）ソフトウェアを移動機へ配信する。

【解決手段】　Ｊａｖａ－ＡＰソフトウェアを起動することができる移動機１６が、ＩＰサーバ装置１３からＡＤＦ２０５を取得し、このＡＤＦ２０５を用いて信頼できる機関（移動パケット通信網１５を管理する通信事業者）が管理する管理サーバ装置１８からＳＤＦ（セキュリティ記述ファイル）２０４を受信し、次いで、ＡＤＦ２０５を用いてＩＰサーバ装置１３からＪａｒファイル２０６を取得し、これらのファイルを内包するＪａｖａ－ＡＰソフトウェアを自身にインストールする。このＪａｖａ－ＡＰソフトウェアを起動することで実現されるＪａｖａ－ＡＰは、ＳＤＦ２０４に内包されているポリシー情報で表される権限の範囲内で動作する。

【選択図】　　図９

出 願 人 履 歴 情 報

識別番号　〔３９２０２６６９３〕

１．変更年月日　２０００年　５月１９日
［変更理由］　名称変更
住　所　東京都千代田区永田町二丁目１１番１号
氏　名　株式会社エヌ・ティ・ティ・ドコモ